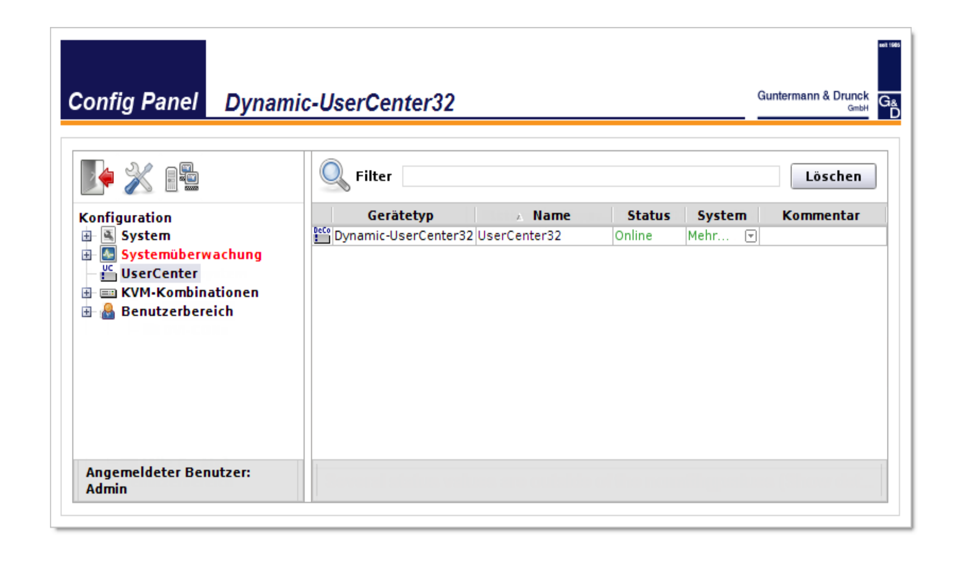


Dynamic-UserCenter 32



DE

Webapplikation »Config Panel«

Konfiguration der Erweiterung

Zu dieser Dokumentation

Diese Dokumentation wurde mit größter Sorgfalt erstellt und nach dem Stand der Technik auf Korrektheit überprüft.

Für die Qualität, Leistungsfähigkeit sowie Marktgängigkeit des G&D-Produkts zu einem bestimmten Zweck, der von dem durch die Produktbeschreibung abgedeckten Leistungsumfang abweicht, übernimmt G&D weder ausdrücklich noch stillschweigend die Gewähr oder Verantwortung.

Für Schäden, die sich direkt oder indirekt aus dem Gebrauch der Dokumentation ergeben, sowie für beiläufige Schäden oder Folgeschäden ist G&D nur im Falle des Vorsatzes oder der groben Fahrlässigkeit verantwortlich.

Gewährleistungsausschluss

G&D übernimmt keine Gewährleistung für Geräte, die

- nicht bestimmungsgemäß eingesetzt wurden.
- nicht autorisiert repariert oder modifiziert wurden.
- schwere äußere Beschädigungen aufweisen, welche nicht bei Lieferungserhalt angezeigt wurden.
- durch Fremdzubehör beschädigt wurden.

G&D haftet nicht für Folgeschäden jeglicher Art, die möglicherweise durch den Einsatz der Produkte entstehen können.

Warenzeichennachweis

Alle Produkt- und Markennamen, die in diesem Handbuch oder in den übrigen Dokumentationen zu Ihrem G&D-Produkt genannt werden, sind Warenzeichen oder eingetragene Warenzeichen der entsprechenden Rechtsinhaber.

Impressum

Version 1.20 – 13.01.2015
Version: 1.11.7

Guntermann & Drunck GmbH
Dortmunder Str. 4a
57234 Wilnsdorf

Germany

Telefon +49 (0) 2739 8901-100
Telefax +49 (0) 2739 8901-120

http://www.GDsys.de
sales@GDsys.de

Inhaltsverzeichnis

Einleitung

Die Webapplikation *Config Panel* bietet eine grafische Benutzeroberfläche zur Konfiguration des KVM-Systems. Sie kann über einen unterstützten Webbrowser (s. Seite 5) bedient werden.

TIPP: Die Webapplikation kann unabhängig von den Standorten der am KVM-System angeschlossenen Geräte und Arbeitsplätze im gesamten Netzwerk eingesetzt werden.

Aufgrund der erweiterten Möglichkeiten der grafischen Benutzeroberfläche ist diese mit folgenden Komfortfunktionen ausgestattet:

- übersichtliche Benutzeroberfläche
- komfortable Bedienung mit Drag & Drop-Funktion
- Überwachung verschiedener Eigenschaften des Systems
- erweiterte Netzwerkfunktionen (Netzfilter, Syslog, …)
- Backup- und Restore-Funktion

Systemvoraussetzungen

Die Webapplikation *Config Panel* ist eine Anwendung für die Java-Plattform. Sie kann über einen unterstützten Webbrowser eines Computers mit installierter Laufzeitumgebung *Java Runtime Environment* gestartet werden.

WICHTIG: Bevor die Webapplikation über den Webbrowser eines Computers verwendet werden kann, ist das Gerät, auf welchem die Webapplikation betrieben wird, zunächst mit dem lokalen Netzwerk zu verbinden (s. Installationsanleitung).

Anschließend sind – sofern nicht bereits erledigt – die auf Seite 6 beschriebenen Netzwerkeinstellungen anzupassen.

Unterstützte Webbrowser

Folgende Webbrowser wurden erfolgreich mit der Webapplikation getestet:

- Internet Explorer 7
- Internet Explorer 8
- Internet Explorer 9
- Mozilla Firefox 35

Java Runtime Environment

Die Webapplikation wird in der Laufzeitumgebung *Java Runtime Environment* (JRE) ausgeführt. Voraussetzung für den Start der Webapplikation ist die Installation der Version 6 (Aktualisierung 19) der Laufzeitumgebung.

Der kostenlose Download ist auf folgender Website möglich:

http://www.oracle.com/technetwork/java/

HINWEIS: Beachten Sie die besonderen Hinweise zum Einsatz der Laufzeitumgebung mit einem 64-bit-Browser unter Windows:

http://www.java.com/de/download/faq/java_win64bit.xml

Erstkonfiguration der Netzwerk-einstellungen

HINWEIS: Im Auslieferungszustand sind folgende Einstellungen vorausgewählt:

- IP-Adresse der *Netzwerkschnittstelle A*: **192.168.0.1**
- IP-Adresse der *Netzwerkschnittstelle B*: Bezug der Adresse via **DHCP**
- globale Netzwerkeinstellungen: Bezug der Einstellungen via **DHCP**

Grundlegende Voraussetzung für den Zugriff auf die Webapplikation ist die Konfiguration der Netzwerkeinstellungen des Gerätes, auf welchem die Webapplikation betrieben wird.

So konfigurieren Sie die Netzwerkeinstellungen vor der Integration des Gerätes in das lokale Netzwerk:

1. Verbinden Sie die Netzwerkschnittstelle eines beliebigen Rechners mit der Schnittstelle *Network A* des Gerätes. Verwenden Sie hierzu ein Twisted-Pair-Kabel der Kategorie 5 (oder höher).
2. Stellen Sie sicher, dass die IP-Adresse der Netwerkschnittstelle des Rechners Teil des Subnetzes ist, welchem auch die IP-Adresse des Gerätes angehört.

   HINWEIS: Verwenden Sie beispielsweise die IP-Adresse *192.168.0.100*.

3. Schalten Sie das Gerät ein.
4. Starten Sie den Webbrowser des Rechners und geben Sie in der Adresszeile die URL **192.168.0.1** ein.
5. Konfigurieren Sie die Netzwerkschnittstelle(n) und die globalen Netzwerkeinstellungen wie im Abschnitt *Netzwerkeinstellungen* auf Seite 17 f. beschrieben.

   WICHTIG: Der Betrieb beider Netzwerkschnittstellen innerhalb eines Subnetzes ist nicht zulässig!

6. Entfernen Sie die Twisted-Pair-Kabelverbindung zwischen dem Rechner und dem Gerät.
7. Integrieren Sie das Gerät in das lokale Netzwerk.

Erste Schritte

In diesem Kapitel lernen Sie die grundlegende Bedienung der Webapplikation kennen.

HINWEIS: Die detaillierte Erläuterung der Funktionen und Konfigurationseinstellungen erfolgt in den folgenden Kapiteln dieses Handbuchs.

Start der Webapplikation

Die Webapplikation kann in einem unterstützten Webbrowser eines Computers mit installierter Laufzeitumgebung *Java Runtime Environment* gestartet werden.

HINWEIS: Informationen zu den Systemvoraussetzungen der Webapplikation finden Sie auf Seite 5.

So starten Sie die Webapplikation:

1. Geben in der Adresszeile folgende URL zum Aufruf der Webapplikation ein:

   https://[IP-Adresse des Gerätes]

HINWEIS: Sie können die Webapplikation alternativ über eine „normale" http-Verbindung (Port 80) starten. In diesem Fall haben Sie keine Möglichkeit, die Gegenseite (über ein Zertifikat) zu authentifizieren.

Sicherheitshinweise des Webbrowsers

Im Gerät, auf welchem die Webapplikation betrieben wird, ist ein SSL-Zertifikat hinterlegt, welches dem Webbrowser bzw. dem Benutzer erlaubt, die Gegenseite zu authentifizieren.

WICHTIG: Ersetzen Sie das im Auslieferungszustand des Geräts enthaltene Zertifikat durch ein individuelles, gerätebezogenes Zertifikat. Die Erstellung eines solchen Zertifikats wird ab Seite 26 beschrieben.

Benutzeranmeldung gegenüber der Webapplikation

Nach der Bestätigung der Zertifikate wird die Login-Maske angezeigt:

So loggen Sie sich in die Webapplikation ein:

1. Geben Sie in die Login-Maske folgende Daten ein:

Benutzername:	Geben Sie Ihren Benutzernamen ein.
Passwort:	Geben Sie das Passwort Ihres Benutzerkontos ein.
Sprachauswahl:	Wählen Sie die Sprache der Benutzeroberfläche: ▪ **(Default):** Standardeinstellung anwenden ▪ **English** ▪ **Deutsch**

2. Klicken Sie auf **Anmelden**.

> **WICHTIG:** Ändern Sie das voreingestellte Passwort des Administratorkontos.
>
> Melden Sie sich hierfür mit dem Administratorkonto in die Webapplikation ein und ändern Sie anschließend das Passwort (s. Seite 68).
>
> Die *voreingestellten* Zugangsdaten zum Administratorkonto lauten:
>
> - **Benutzername:** Admin
> - **Passwort:** 4658

Bedienung der Webapplikation

Die Benutzeroberfläche

Die Benutzeroberfläche der Webapplikation besteht aus vier Hauptbereichen:

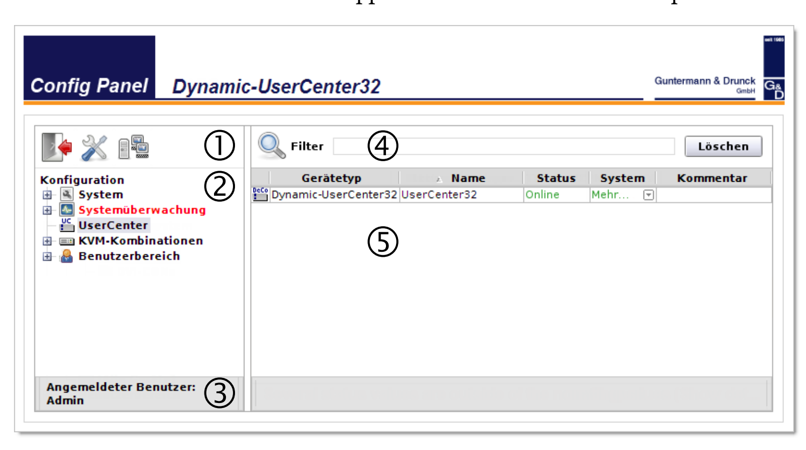


Abbildung 1: Benutzeroberfläche der Webapplikation

Die unterschiedlichen Bereiche der Benutzeroberfläche dienen verschiedenen Aufgaben. Die folgende Tabelle listet den Anwendungszweck jedes Bereichs auf:

Symbolleiste ①:	Über die Symbolleiste können Sie jederzeit die aktive Sitzung beenden und haben Zugriff auf die Grundkonfiguration der Webapplikation.
Strukturansicht ②:	Die Strukturansicht enthält eine hierarchische Auflistung der Einstellungsmöglichkeiten.
Benutzer-Anzeige ③:	Anzeige des an Webapplikation angemeldeten Benutzers
Filterfunktion ④:	Die Filterfunktion kann genutzt werden, um die in der Hauptansicht angezeigten Elemente einzugrenzen. Geben Sie im Textfeld einen Teil des Namens des gesuchten Elements ein. Daraufhin werden ausschließlich solche Elemente in der Hauptansicht angezeigt, die diesen Text im Namen enthalten. Die Groß-/Kleinschreibung der Namen wird bei der Filterung ignoriert. Um die Filterung aufzuheben, klicken Sie auf **Löschen**.
Hauptansicht ⑤:	Nach der Auswahl eines Elementes der Strukturansicht ② werden hier die untergeordneten Elemente dargestellt.

TIPP: In der Hauptansicht der Zweige **UserCenter** und **KVM-Kombinationen** können Sie zwischen dem *Monitoring*- und dem *Info*-Modus umschalten.

Im *Monitoring-Modus* werden in der Hauptansicht die Werte der überwachten Elemente angezeigt. Im *Info-Modus* werden wichtige Informationen, wie beispielsweise die Firmware-Version, die IP- und MAC-Adresse(n) der Geräte angezeigt.

Klicken Sie mit der rechten Maustaste in die Tabelle und wählen Sie **Spaltenansicht > Monitoring** bzw. **Informationen**, um den gewünschten Modus zu aktivieren.

Häufig verwendete Schaltflächen

Die Benutzeroberfläche verwendet verschiedene Schaltflächen zur Durchführung von Operationen. Über die Bezeichnungen und Funktionen der in vielen Dialogmasken verwendeten Schaltflächen informiert Sie die folgende Tabelle:

Neu laden:	Erneutes Auslesen der Werte eines Dialoges aus der Datenbank des Systems. Von Ihnen durchgeführte Änderungen der Werte werden hierbei überschrieben.
OK:	Speicherung der eingegebenen Daten. *Der geöffnete Dialog wird geschlossen.*
Übernehmen:	Speicherung der eingegebenen Daten. *Der geöffnete Dialog wird weiterhin angezeigt.*
Abbrechen:	Die von Ihnen eingegebenen Daten werden verworfen und der Dialog geschlossen.

Drucken:	Aufruf des Druck-Dialog zur Auswahl des Druckers, der Seitenausrichtung und anderer Einstellungen. Nach der Auswahl der Einstellungen können die Informationen des Dialoges gedruckt werden.
Schließen:	Eingabe beenden und geöffneten Dialog schließen.

Abmeldung eines Benutzers

Mit der *Logout*-Funktion beenden Sie die aktive Sitzung der Webapplikation.

WICHTIG: Verwenden Sie immer die *Logout*-Funktion nach Abschluss Ihrer Arbeit mit der Webapplikation.

Die Webapplikation wird so gegen unautorisierten Zugriff geschützt.

So beenden Sie die aktive Sitzung der Webapplikation:

1. Klicken Sie auf das **Logout**-Symbol (s. Abbildung rechts), um die aktive Sitzung der Webapplikation zu beenden.

   Nach der erfolgreichen Abmeldung des Benutzers wird der *Login*-Dialog angezeigt.

Standardsprache der Webapplikation auswählen

So ändern Sie die Standardsprache der Webapplikation:

1. Klicken Sie im Strukturbaum auf **System**.
2. Doppelklicken Sie in der Hauptansicht auf **Konfiguration**.
3. Klicken Sie auf den Reiter **System**.
4. Wählen Sie im Feld **Sprache** die Standardsprache aus, die alle Benutzer der Webapplikation angezeigt bekommen, die die Sprache *(Default)* auswählen:

   - **Deutsch**
   - **English**

5. Klicken Sie auf **OK**, um die Daten zu speichern.

Hash-Algorithmus für die Speicherung der Passwörter auswählen

Die Passwörter der Benutzer werden standardmäßig in Form von MD5-Hashwerte in der Datenbank gespeichert.

Falls gewünscht, können Sie den Hash-Algorithmus auf **bcyrpt** umstellen.

HINWEIS: Der Hash-Algorithmus **bcrypt** wird seit der Firmware-Version 1.2.000 unterstützt.

Aktualisieren Sie ggf. die Firmware eines Matrixswitches, bevor Sie ein Backup mit enthaltenen **bcrypt**-Hashwerten wiederherstellen.

So ändern Sie Hash-Alogrithmus für die Speicherung der Passwörter:

1. Klicken Sie im Strukturbaum auf **System**.
2. Doppelklicken Sie in der Hauptansicht auf **Konfiguration**.
3. Klicken Sie auf den Reiter **System**.
4. Wählen Sie im Feld **Hash-Algorithmus** den gewünschten Algorithmus aus:

   - **MD5**
   - **bcrypt**

5. Klicken Sie auf **OK**, um die Daten zu speichern.

Versionsnummer der Webapplikation anzeigen

So zeigen Sie die Versionsnummer der Webapplikation an:

1. Klicken Sie im Strukturbaum auf **System > Information**.
2. Doppelklicken Sie in der Hauptansicht auf **Allgemein**.
3. Klicken Sie auf **Schließen**, um das Fenster zu schließen.

Verwaltung der »Dynamic Ports«

In der Standardeinstellung sind die *Dynamic Ports* in acht Gruppen aufgeteilt. Jede Gruppe erlaubt den Anschluss eines Target-Moduls und dreier Matrixswitches.

Der folgende Screenshot stellt die Standardkonfiguration der Ports visuell dar:

UC Dynamic Ports

2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32
1	1	5	5	9	9	13	13	17	17	21	21	25	25	29	29
1	1	5	5	9	9	13	13	17	17	21	21	25	25	29	29
1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31

Pro Port werden folgende Information angezeigt:



Das Computersymbol kennzeichnet *CPU*-Ports.
Hieran schließen Sie ein Target-Modul der *DVI-CPU*-Serie an.



Das Cluster-Symbol kennzeichnet *Cluster*-Ports.
Hieran schließen Sie einen Matrixswitch der *DVICenter*-Serie an.



Jeder zugeordnete Port ist Mitglied einer Gruppe. Die Gruppennummer wird unterhalb der Computer- und Cluster-Symbole angezeigt.
Sie resultieren aus der Nummer des *CPU-Ports* der Gruppe.

»Dynamic Ports« konfigurieren

Die Ports der Erweiterung *Dynamic-UserCenter 32* können Sie individuell gruppieren und zuordnen. Jede Gruppe besteht aus einem *CPU-Port*, an den ein Target-Modul angeschlossen wird. Zusätzlich fügen Sie mindestens zwei *Cluster-Ports* der Gruppe hinzu. An diese Ports werden die Matrixswitches angeschlossen, die das Target-Modul aufschalten können.

So konfigurieren Sie die »Dynamic Ports«:

1. Klicken Sie auf das **Dynamic Port**-Symbol (s. Abbildung rechts) in der Symbolleiste der Webapplikation.



2. Im Konfigurationsdialog wird eine **Grafik unter der Tabelle** (Standardansicht) angezeigt. Sowohl über die Grafik als auch über die Tabelle können Sie die *Dynamic Ports* konfigurieren.

   Aktivieren Sie gegebenenfalls eine alternative Ansicht: **Nur Tabelle**, **Grafik neben Tabelle** oder **Nur Grafik**.
3. Falls gewünscht, klicken Sie auf die Schaltfläche **Vordefinierten Konfigurationen**. Hier können Sie eines der häufig verwendeten Port-Layouts (**1:3**, **1:7** oder **1:15**) auswählen, oder die Zuordnung aller Ports zurücksetzen (**Nicht zugeordnet**).
4. Das aktuelle Port-Layout oder eine der vordefinierten Konfigurationen können Sie individuell anpassen. Die Tabelle listet die möglichen Aktionen auf.

> **TIPP:** Die Mehrfachauswahl von Ports ist bei gleichzeitiger Betätigung der **Shift**- bzw. der **Strg**-Taste mit der linken Maustaste möglich.

> **TIPP:** Bei der Ausführung der Aktionen in der Tabelle können Sie alternativ die »Drag and Drop«-Methode nutzen.

Aktion in Grafik ausführen	Aktion in Tabelle ausführen
EINE NEUE PORT-GRUPPE ERSTELLEN	
▪ Rechtsklicken Sie auf einen unzugeordneten Port, den Sie als *CPU-Port* der neuen Gruppe nutzen möchten. ▪ Klicken Sie auf den Eintrag **Neue Gruppe** im Kontextmenü.	▪ Klicken Sie in der linken Spalte auf den zu erstellenden *CPU-Port* der neuen Port-Gruppe. ▪ Klicken Sie auf .
EINEN CLUSTER-PORT EINER PORT-GRUPPE ZUWEISEN	
▪ Rechtsklicken Sie auf einen unzugeordneten Port, den Sie als *Cluster-Port* einer Gruppe hinzufügen möchten. ▪ Klicken Sie auf den Eintrag **Zuordnen** im Kontextmenü. ▪ Wählen Sie den *CPU-Port*, in dessen Gruppe Sie den *Cluster-Port* hinzufügen möchten.	▪ Klicken Sie in der linken Spalte auf den hinzuzufügenden *Cluster-Port*. ▪ Klicken Sie in der rechten Spalte auf den Gruppennamen oder einen Port der Gruppe, der Sie den *Cluster-Port* hinzufügen möchten. ▪ Klicken Sie auf .

EINEN CLUSTER-PORT AUS EINER PORT-GRUPPE ENTFERNEN	
▪ Rechtsklicken Sie auf den *Cluster-Port*, den Sie aus einer Gruppe entfernen möchten. ▪ Klicken Sie auf den Eintrag **Aus Gruppe entfernen** im Kontextmenü.	▪ Klicken Sie in der rechten Spalte auf den *Cluster-Port*, den Sie aus einer Gruppe entfernen möchten. ▪ Klicken Sie auf .
EINE GRUPPE LÖSCHEN ‣ Achtung: Alle Ports einer Port-Gruppe werden gelöscht!	
▪ Rechtsklicken Sie auf den *CPU-Port*, dessen Gruppe Sie löschen möchten. ▪ Klicken Sie auf den Eintrag **Gruppe löschen** im Kontextmenü.	▪ Klicken Sie in der rechten Spalte auf den *CPU-Port*, dessen Gruppe Sie löschen möchten. ▪ Klicken Sie auf .

TIPP: Verwenden Sie die Schaltfläche **Drucken**, um eine detaillierte Auflistung der Ports zu drucken.

5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

WICHTIG: Nach der Änderung der Portzuordnung startet das Gerät neu!

6. Klicken Sie auf das **Logout**-Symbol (s. Abbildung rechts), um die aktive Sitzung der Webapplikation zu beenden.



Anzeigemodi der »Dynamic Ports«-LEDs ändern

In der Standardeinstellung des Gerätes signalisieren die LEDs der *Dynamic Ports* den Status der Schnittstelle.

Zur Erleichterung der Installation können die LEDs der *Dynamic Ports* in den *Port-Modus* geschaltet werden. Die *Dynamic Ports* zum Anschluss der Matrixswitches bzw. der Arbeitsplatzmodule werden in diesem Modus durch das Aufleuchten von LEDs in grüner bzw. gelber Farbe gekennzeichnet.

So aktivieren Sie die Signalisierung des Port-Modus der *Dynamic Ports*:

1. Klicken Sie im Strukturbaum auf **UserCenter**.
2. Klicken Sie mit der rechten Maustaste auf das Gerät und anschließend auf **Dynamic Port-LEDs > Port-Typ anzeigen** im Kontextmenü.

3. Wählen Sie **System**, um die Port-Modi aller Ports anzuzeigen oder wählen Sie die Port-Gruppe aus, auf die Sie die Signalisierung beschränken möchten.

   Die LEDs der *Dynamic Ports* signalisieren den aktuellen Port-Modus:

LED	Port-Modus
gelb	Anschluss von Matrixswitches
grün	Anschluss von Target-Modulen

> **HINWEIS:** Während der Signalisierung der Port-Modi blinken die *Identification*-LEDs an der Front- und der Rückseite des Gerätes.

So aktivieren Sie die Signalisierung des Schnittstellenstatus der *Dynamic Ports*:

1. Klicken Sie im Strukturbaum auf **UserCenter**.
2. Klicken Sie mit der rechten Maustaste auf das Gerät und anschließend auf **Dynamic Port-LEDs > Status anzeigen** im Kontextmenü.
3. Wählen Sie **System**, um den Status aller Ports anzuzeigen oder wählen Sie die Port-Gruppe aus, auf die Sie die Signalisierung beschränken möchten.

   Die LEDs der *Dynamic Ports* signalisieren jetzt den aktuellen Status der einzelnen Ports (siehe Installationshandbuch).

Direktanschluss von Arbeitsplatzmodulen erlauben oder verbieten

In der Standardeinstellung des Gerätes ist anstelle der Matrixswitches auch der Anschluss von Arbeitsplatzmodulen der *DVI-CON*-Serie an die *Cluster-Ports* erlaubt.

Ändern Sie die Einstellung **Direkt-Konsolen** in der Webapplikation, falls Sie dies verhindern möchten.

So erlauben bzw. verbieten Sie den Direktanschluss von Arbeitsplatzmodulen:

1. Klicken Sie im Strukturbaum auf **UserCenter**.
2. Klicken Sie mit der rechten Maustaste auf das zu konfigurierende Gerät und anschließend auf **Konfiguration** im Kontextmenü.

3. Wählen Sie zwischen folgenden Optionen der Einstellung **Direkt-Konsolen**:

Erlaubt:	Der Anschluss von Arbeitsplatzmodulen der DVI-CON-Serie an die *Cluster-Ports* ist erlaubt. Die Aufschaltung auf ein Arbeitsplatzmodul ist möglich.
Verboten:	Der Anschluss von Arbeitsplatzmodulen der *DVI-CON*-Serie an die *Cluster-Ports* ist verboten. Beim Versuch der Aufschaltung auf ein Arbeitsplatzmodul wird eine Meldung ausgegeben, dass kein Matrixswitch gefunden wurde.

4. Klicken Sie auf **OK**, um den Dialog zu verlassen.

Grundkonfiguration der Webapplikation

Über das Werkzeugsymbol in der Symbolleiste haben Sie Zugriff auf die Grundkonfiguration der Webapplikation.

Netzwerkeinstellungen

Die Geräte mit integrierter Webapplikation sind mit zwei Netzwerkschnittstellen (*Network A* und *Network B*) ausgestattet. Die Netzwerkschnittstellen erlauben die Integration eines Gerätes in bis zu zwei separate Netzwerke.

> **WICHTIG:** Beachten Sie die separaten Anweisungen zur *Erstkonfiguration der Netzwerkeinstellungen* auf Seite 6.

Konfiguration der Netzwerkschnittstellen

Zur Anbindung des Gerätes an ein lokales Netzwerk sind die Einstellungen des Netzwerks zu konfigurieren.

> **HINWEIS:** Im Auslieferungszustand sind folgende Einstellungen vorausgewählt:
> - IP-Adresse der *Netzwerkschnittstelle A*: **192.168.0.1**
> - IP-Adresse der *Netzwerkschnittstelle B*: Bezug der Adresse via **DHCP**
> - globale Netzwerkeinstellungen: Bezug der Einstellungen via **DHCP**

So konfigurieren Sie die Einstellungen einer Netzwerkschnittstelle:

> **WICHTIG:** Der Betrieb beider Netzwerkschnittstellen innerhalb eines Subnetzes ist nicht zulässig!

> **HINWEIS:** Der *Link Local*-Adressraum 169.254.0.0/16 ist gemäß RFC 3330 für die interne Kommunikation zwischen Geräten reserviert. Die Zuordnung einer IP-Adresse dieses Adressraums ist nicht möglich!

1. Klicken Sie in der Symbolleiste auf das Werkzeugsymbol.
2. Klicken Sie auf die Reiter **Netzwerk > Schnittstellen**.
3. Erfassen Sie im Abschnitt **Schnittstelle A** oder **Schnittstelle B** folgende Daten:

Betriebsmodus:	Wählen Sie den Betriebsmodus der **Schnittstelle A** bzw. **Schnittstelle B** aus: ▪ **Aus:** Netzwerkschnittstelle ausschalten. ▪ **Statisch:** Es wird eine statische IP-Adresse zugeteilt. ▪ **DHCP:** Bezug der IP-Adresse von einem DHCP-Server. ▪ **Link-Aggregation aktiv:** Diese Schnittstelle wurde zu einer Netzwerkschnittstellen-Gruppe hinzugefügt. *Konfigurieren Sie die Netzwerkschnittstellen in diesem Fall über den Reiter »Link-Aggregation«.*

IP-Adresse:	Geben Sie – nur bei Auswahl des Betriebsmodus *Statisch* – die IP-Adresse der Schnittstelle an.
Netzmaske:	Geben Sie – nur bei Auswahl des Betriebsmodus *Statisch* – die Netzmaske des Netzwerkes an.
Verbindungstyp:	Wählen Sie aus, ob der Verbindungstyp automatisch (**Auto**) mit der Gegenstelle ausgehandelt werden soll oder ob einer der verfügbaren Typen fest einzustellen ist.

4. Klicken Sie auf **OK**, um die Daten zu speichern.

Konfiguration der globalen Netzwerkeinstellungen

Die globalen Netzwerkeinstellungen stellen auch in komplexen Netzwerken sicher, dass die Webapplikation aus allen Teilnetzwerken erreichbar ist.

So konfigurieren Sie die globalen Netzwerkeinstellungen:

1. Klicken Sie in der Symbolleiste auf das Werkzeugsymbol.
2. Klicken Sie auf die Reiter **Netzwerk** > **Schnittstellen**.
3. Erfassen Sie folgende Daten im Abschnitt **Globale Netzwerkeinstellungen**:

Betriebsmodus:	Wählen Sie den gewünschten Betriebsmodus: ▪ **Statisch:** Verwendung von statischen Einstellungen. ▪ **DHCP:** Bezug der Einstellungen von einem DHCP-Server.
Im Betriebsmodus *DHCP* werden die folgenden Einstellungen automatisch bezogen. Eine Eingabe ist nicht möglich.	
Host-Name:	Geben Sie den Host-Namen des Gerätes ein.
Domäne:	Geben Sie die Domäne an, welcher das Gerät angehören soll.
Gateway:	Geben Sie die IP-Adresse des Gateways an.
DNS-Server 1:	Geben Sie die IP-Adresse des DNS-Servers an.
DNS-Server 2:	Geben Sie *optional* die IP-Adresse eines weiteren DNS-Servers an.

4. Klicken Sie auf **OK**, um die Daten zu speichern.

Ausfallsicherheit der Netzwerkverbindung durch Link-Aggregation erhöhen

In der Standardeinstellung können beide Netzwerkschnittstellen parallel eingesetzt werden, um beispielsweise aus zwei verschiedenen Netzwerksegmenten auf die Webapplikation zuzugreifen.

Zur Erhöhung der Ausfallsicherheit können die Netzwerkschnittstellen via *Link-Aggregation* zu einer Gruppe zusammengefasst werden. Innerhalb der Gruppe ist stets nur eine Schnittstelle aktiv. Eine andere Schnittstelle wird nur aktiv, falls die aktive Schnittstelle ausfällt.

Zur Überwachung der Schnittstellen stehen zwei verschiedene Modi zur Verfügung:

- **MII-Modus:** Der Carrier-Status der Netzwerkschnittstelle wird über das *Media Independent Interface* überwacht. In diesem Modus wird lediglich die Funktionalität der Netzwerkschnittstelle geprüft.
- **ARP-Modus:** Über das *Address-Resolution-Protokoll* werden Anfragen an ein ARP-Target im Netzwerk gesendet. Die Antwort des ARP-Targets bestätigt sowohl die Funktionalität der Netzwerkschnittstelle, als auch eine einwandfreie Netzwerkverbindung zum ARP-Target.

Ist das ARP-Target zwar mit dem Netzwerk verbunden, aber temporär offline, können die Anfragen nicht beantwortet werden. Bestimmen Sie daher mehrere ARP-Targets, um auch bei Ausfall eines ARP-Targets eine Rückmeldung mindestens eines Targets zu erhalten.

HINWEIS: Die Kombination des **MII-** und des **ARP-Modus** ist nicht möglich!

So konfigurieren Sie die Einstellungen einer Netzwerkschnittstellen-Gruppe:

HINWEIS: Der *Link Local*-Adressraum 169.254.0.0/16 ist gemäß RFC 3330 für die interne Kommunikation zwischen Geräten reserviert. Die Zuordnung einer IP-Adresse dieses Adressraums ist nicht möglich!

1. Klicken Sie in der Symbolleiste auf das Werkzeugsymbol.
2. Klicken Sie auf die Reiter **Netzwerk > Link-Aggregation**.
3. Erfassen Sie im Abschnitt **Netzwerk** folgende Daten:

Name:	Geben Sie den gewünschten Namen der Netzwerkschnittstellen-Gruppe ein.
Betriebsmodus:	Wählen Sie den Betriebsmodus der Netzwerkschnittstellen-Gruppe aus: ▪ **Aus:** Link-Aggregation ausschalten. *Konfigurieren Sie die Netzwerkschnittstellen in diesem Fall über den Reiter »Schnittstellen«.* ▪ **Statisch:** Es wird eine statische IP-Adresse zugeteilt. ▪ **DHCP:** Bezug der IP-Adresse von einem DHCP-Server.
IP-Adresse:	Geben Sie – nur bei Auswahl des Betriebsmodus *Statisch* – die IP-Adresse der Schnittstelle an.
Netzmaske:	Geben Sie – nur bei Auswahl des Betriebsmodus *Statisch* – die Netzmaske des Netzwerkes an.

4. Erfassen Sie im Abschnitt **Parameter** folgende Daten:

Primärer Slave:	Wählen Sie, ob der Datenverkehr bevorzugt über die Schnittstelle *Network A* (**Schnittstelle A**) bzw. *Network B* (**Schnittstelle B**) erfolgen soll. Sobald die ausgewählte Schnittstelle verfügbar ist, wird diese Schnittstelle für den Datenverkehr verwendet. Wählen Sie die Option **Keiner**, wird der Datenverkehr über eine beliebige Schnittstelle gesendet. Eine Umschaltung erfolgt nur, wenn die aktive Schnittstelle ausfällt.
Link-Monitoring:	Wählen Sie, ob der **MII-** oder der **ARP-Modus** (s. Erläuterung oben) zum Monitoring der Schnittstelle verwendet werden soll.
MII-Down-Delay:	Wartezeit in Millisekunden, bevor eine ausgefallene Netzwerkschnittstelle deaktiviert wird. Der eingegebene Wert muss ein Vielfaches von 100 ms (der MII-Link-Monitoring-Frequenz) sein.
MII-Up-Delay:	Wartezeit in Millisekunden, bevor eine wiederhergestellte Netzwerkschnittstelle aktiviert wird. Der eingegebene Wert muss ein Vielfaches von 100 ms (der MII-Link-Monitoring-Frequenz) sein.
ARP-Intervall:	Geben Sie das Intervall (100 bis 10.000 Millisekunden) ein, nach welchem eine Prüfung auf eingegangene ARP-Pakete der Netzwerkschnittstellen erfolgt.
ARP-Validierung:	Die Validierung stellt sicher, dass das ARP-Paket für eine bestimmte Netzwerkschnittstelle von einem der angegebenen ARP-Targets generiert wurde. Wählen Sie, ob bzw. welche der eingehenden ARP-Pakete validiert werden sollen: ▪ **Keine:** Die ARP-Pakete werden nicht validiert (Standard). ▪ **Aktiv:** Ausschließlich die ARP-Pakete der aktiven Netzwerkschnittstelle werden validiert. ▪ **Backup:** Ausschließlich die ARP-Pakete der inaktiven Netzwerkschnittstelle werden validiert. ▪ **Alle:** Die ARP-Pakete aller Netzwerkschnittstellen der Gruppe werden validiert.
ARP-Target:	Die Tabelle enthält eine Liste aller konfigurierten ARP-Targets. Verwenden Sie die Schaltflächen **Hinzufügen**, **Ändern** und **Löschen**, um die ARP-Targets zu verwalten.

5. Klicken Sie auf **OK**, um die Daten zu speichern.

Status der Netzwerkschnittstellen auslesen

Den aktuellen Status der beiden Netzwerkschnittstellen des Gerätes können Sie in der Webapplikation auslesen.

So ermitteln Sie den Status der Netzwerkschnittstellen:

1. Klicken Sie in der Symbolleiste auf das Werkzeugsymbol.
2. Klicken Sie auf die Reiter **Netzwerk > Link-Status**.
3. In den Abschnitten **Schnittstelle A** und **Schnittstelle B** werden Ihnen folgende Daten angezeigt:

Link detected:	Verbindung zum Netzwerk hergestellt (**ja**) oder unterbrochen (**nein**).
Auto-negotiation:	Die Übertragungsgeschwindigkeit und des Duplex-Verfahren wurde automatisch (**ja**) oder manuell vom Administrator konfigurert (**nein**).
Speed:	Übertragungsgeschwindigkeit
Duplex:	Duplexverfahren (**full** bzw. **half**)

4. Klicken Sie auf **OK**, um das Fenster zu schließen.

Netzfilterregeln einrichten und administrieren

Im Auslieferungszustand der Geräte haben alle Netzwerkrechner Zugriff auf die Webapplikation *Config Panel* (offener Systemzugang).

HINWEIS: Der offene Systemzugang erlaubt uneingeschränkte Verbindungen über die Ports 80/TCP (HTTP), 443/TCP (HTTPS) und 161/UDP (SNMP).

Sobald eine Netzfilterregel erstellt ist, wird der offene Systemzugang deaktiviert und alle eingehenden Datenpakete mit den Netzfilterregeln verglichen. Die Liste der Netzfilterregeln wird hierbei in der gespeicherten Reihenfolge abgearbeitet. Sobald eine Regel zutrifft, wird die entsprechende Aktion ausgeführt und die nachfolgenden Regeln werden ignoriert.

Neue Netzfilterregel erstellen

So erstellen Sie eine neue Netzfilterregel:

1. Klicken Sie in der Symbolleiste auf das Werkzeugsymbol.
2. Klicken Sie auf die Reiter **Netzwerk > Netzfilter**.
3. Erfassen Sie folgende Daten:

Schnittstelle:	Wählen Sie im Pull-Down-Menü aus, auf welchen Netzwerkschnittstellen die Datenpakete abgefangen und manipuliert werden sollen: ▪ **Alle** ▪ **Schnittstelle A** ▪ **Schnittstelle B** ▪ **[Name einer Netzwerkschnittstellen-Gruppe]**
Option:	Wählen Sie im Pull-Down-Menü aus, wie die Absenderinformation der Regel zu interpretieren ist: ▪ **Normal:** Die Regel gilt für Datenpakete, deren Absenderinformation der in der Regel angegebenen IP-Adresse bzw. MAC-Adresse entspricht. ▪ **Invertiert:** Die Regel gilt für Datenpakete, deren Absenderinformation *nicht* der in der Regel angegebenen IP-Adresse bzw. MAC-Adresse entspricht.
IP-Adresse/ Netzmaske:	Geben Sie die IP-Adresse der Datenpakete oder – durch Verwendung des Feldes **Netzmaske** – den Adressraum der IP-Adressen ein. **Beispiele:** ▪ **192.168.150.187:** nur die IP-Adresse 192.168.150.187 ▪ **192.168.150.0/24:** IP-Adressen des Raums 192.168.150.x ▪ **192.168.0.0/16:** IP-Adressen des Raums 192.168.x.x ▪ **192.0.0.0/8:** IP-Adressen des Raums 192.x.x.x ▪ **0.0.0.0/0:** alle IP-Adressen
HINWEIS: Innerhalb einer Regel können wahlweise die *IP-Adresse* und/ oder eine *MAC-Adresse* angegeben werden.	
MAC-Adresse:	Geben Sie die MAC-Adresse ein, welche in dieser Filterregel zu berücksichtigen ist.
HINWEIS: Innerhalb einer Regel können wahlweise die *IP-Adresse* und/ oder eine *MAC-Adresse* angegeben werden.	

Filterregel:	▪ **Drop:** Datenpakete, deren Absenderinformation mit der IP-Adresse bzw. MAC-Adresse übereinstimmt, werden *nicht* verarbeitet. ▪ **Accept:** Datenpakete, deren Absenderinformation mit der IP-Adresse bzw. MAC-Adresse übereinstimmt, werden verarbeitet.

4. Klicken Sie auf **Hinzufügen**, um die Daten in einer neuen Filterregel zu speichern.

   Die neue Filterregel wird an das Ende der Liste der bestehenden Filterregeln angefügt.

5. Klicken Sie auf **OK**, um den Dialog zu verlassen.

HINWEIS: Die neue Netzfilterregel wird nicht auf aktive Verbindungen angewendet. Starten Sie das Gerät neu, wenn Sie die Trennung der aktiven Verbindungen und die anschließende Anwendung aller Regeln wünschen.

Bestehende Netzfilterregel bearbeiten

So bearbeiten Sie eine bestehende Netzfilterregel:

1. Klicken Sie in der Symbolleiste auf das Werkzeugsymbol.
2. Klicken Sie auf die Reiter **Netzwerk > Netzfilter**.
3. Markieren Sie in der Liste der bestehenden Netzfilterregeln die zu ändernde Regel.
4. Die aktuellen Einstellungen der Regel werden im oberen Bereich des Dialogs angezeigt. Prüfen und ändern Sie die folgenden Daten.

Interface:	Wählen Sie im Pull-Down-Menü aus, auf welchen Netzwerkschnittstellen die Datenpakete abgefangen und manipuliert werden sollen: ▪ **Alle** ▪ **Netzwerk A** ▪ **Netzwerk B**
Option:	Wählen Sie im Pull-Down-Menü aus, wie die Absenderinformation der Regel zu interpretieren ist: ▪ **Normal:** Die Regel gilt für Datenpakete, deren Absenderinformation der in der Regel angegebenen IP-Adresse bzw. MAC-Adresse entspricht. ▪ **Invertiert:** Die Regel gilt für Datenpakete, deren Absenderinformation *nicht* der in der Regel angegebenen IP-Adresse bzw. MAC-Adresse entspricht.

IP-Adresse/ Netzmaske:	Geben Sie die IP-Adresse der Datenpakete oder – durch Verwendung des Feldes **Netzmaske** – den Adressraum der IP-Adressen ein. **Beispiele:** ▪ **192.168.150.187:** nur die IP-Adresse 192.168.150.187 ▪ **192.168.150.0/24:** IP-Adressen des Raums 192.168.150.x ▪ **192.168.0.0/16:** IP-Adressen des Raums 192.168.x.x ▪ **192.0.0.0/8:** IP-Adressen des Raums 192.x.x.x ▪ **0.0.0.0/0:** alle IP-Adressen
Innerhalb einer Regel können wahlweise die *IP-Adresse* und/oder eine *MAC-Adresse* angegeben werden.	
MAC-Adresse:	Geben Sie die MAC-Adresse ein, welche in dieser Filterregel zu berücksichtigen ist.
Innerhalb einer Regel können wahlweise die *IP-Adresse* und/oder eine *MAC-Adresse* angegeben werden.	
Filterregel:	▪ **Drop:** Datenpakete, deren Absenderinformation mit der IP-Adresse bzw. MAC-Adresse übereinstimmt, werden *nicht* verarbeitet. ▪ **Accept:** Datenpakete, deren Absenderinformation mit der IP-Adresse bzw. MAC-Adresse übereinstimmt, werden verarbeitet.

5. Klicken Sie auf **Ändern**, um die von Ihnen geänderten Daten zu speichern.
6. Klicken Sie auf **OK**, um den Dialog zu verlassen.

HINWEIS: Die geänderte Netzfilterregel wird nicht auf aktive Verbindungen angewendet. Starten Sie das Gerät neu, wenn Sie die Trennung der aktiven Verbindungen und die anschließende Anwendung aller Regeln wünschen.

Bestehende Netzfilterregeln löschen

So löschen Sie bestehende Netzfilterregeln:

1. Klicken Sie in der Symbolleiste auf das Werkzeugsymbol.
2. Klicken Sie auf die Reiter **Netzwerk > Netzfilter**.
3. Markieren Sie in der Liste der bestehenden Netzfilterregeln die zu löschende Regel.
4. Klicken Sie auf **Entfernen**.
5. Bestätigen Sie die erscheinende Sicherheitsabfrage durch Klick auf **Ja** oder brechen Sie den Vorgang durch Klick auf **Nein** ab.
6. Klicken Sie auf **OK**, um den Dialog zu verlassen.

Reihenfolge bzw. Priorität der Netzfilterregeln ändern

Die Liste der Netzfilterregeln wird in der gespeicherten Reihenfolge abgearbeitet. Sobald eine Regel zutrifft, wird die entsprechende Aktion ausgeführt und die nachfolgenden Regeln werden ignoriert.

WICHTIG: Achten Sie – insbesondere beim Hinzufügen neuer Regeln – auf die Reihenfolge bzw. Priorität der einzelnen Regeln.

So ändern Sie die Reihenfolge/Priorität der bestehenden Netzfilterregeln:

1. Klicken Sie in der Symbolleiste auf das Werkzeugsymbol.
2. Klicken Sie auf die Reiter **Netzwerk > Netzfilter**.
3. Markieren Sie in der Liste der bestehenden Netzfilterregeln jene Regel, deren Reihenfolge/Proritä Sie ändern möchten.
4. Klicken Sie auf (*Pfeil auf*), um die Priorität zu erhöhen oder auf (*Pfeil ab*), um die Priorität zu verringern.
5. Klicken Sie auf **OK**, um den Dialog zu verlassen.

Erstellung eines SSL-Zertifikats

Die Erstellung eines SSL-Zertifikats kann beispielsweise mit der freien Implementierung des SSL/TLS-Protokolls *OpenSSL* erfolgen.

Detaillierte Informationen zur Bedienung von OpenSSL finden Sie auf folgenden Websites:

- OpenSSL-Projekt: **http://www.openssl.org/**
- Win32 OpenSSL: **http://www.slproweb.com/products/Win32OpenSSL.html**

> **WICHTIG:** Voraussetzung für die Erstellung eines SSL-Zertifikats ist die Software OpenSSL. Folgen Sie ggf. den Anleitungen auf den oben genannten Websites, um die Software zu installieren.

Die Anleitung auf den folgenden Seiten erläutert *exemplarisch* die Erstellung eines SSL-Zertifikates.

Besonderheiten für komplexe KVM-Systeme

Falls innerhalb eines KVM-Systems verschiedene G&D-Geräte miteinander kommunizieren sollen, ist bei der Erstellung von Zertifikaten für diese Geräte das identische *Certificate Authority*-Zertifikat (s. Seite 26) zu verwenden.

Alternativ kann bei allen Geräten auch die identische PEM-Datei (s. Seite 29) verwendet werden. In diesem Fall sind alle Merkmale der Zertifikate identisch.

Erzeugen eines Certificate Authority-Zertifikats

Das *Certificate Authority*-Zertifikat berechtigt den Inhaber digitale Zertifikate (z. B. für einen Matrixswitch) zu erstellen.

So erstellen Sie zunächst einen Schlüssel für das Certificate Authority-Zertifikat:

> **WICHTIG:** Der im folgenden Schritt zu erstellende Schlüssel wird *nicht* verschlüsselt. Lesen Sie ggf. in der Dokumentation von OpenSSL nach, um zu erfahren wie ein verschlüsselter Schlüssel erstellt werden kann!

1. Geben Sie folgenden Befehl in der Eingabeaufforderung ein und betätigen Sie anschließend die **Eingabetaste**:

```
openssl genrsa -out ca.key 4096
```

2. Der Schlüssel wird durch OpenSSL erstellt und unter dem Dateinamen *ca.key* gespeichert.

So erstellen Sie das Certificate Authority-Zertifikat:

1. Geben Sie folgenden Befehl in der Eingabeaufforderung ein und betätigen Sie anschließend die **Eingabetaste**:

```
openssl req -new -x509 -days 3650 -key ca.key -out ca.crt
```

2. OpenSSL erfragt nun einige Daten, die in das Zertifikat integriert werden.

   Nachfolgend werden die verschiedenen Felder und eine exemplarische Eingabe aufgeführt:

Feld	Beispiel
Country Name (2 letter code)	DE
State or Province Name	NRW
Locality Name (eg, city)	Wilnsdorf
Organization Name (eg, company)	Guntermann & Drunck GmbH
Organizational Unit Name (eg, section)	
Common Name (eg, YOUR name)	Guntermann & Drunck GmbH
Email Address	

   WICHTIG: In der Zeile *Common Name* darf *nicht* die IP-Adresse des Gerätes eingegeben werden!

   Geben Sie die von Ihnen gewünschten Daten ein und bestätigen Sie jede Eingabe durch Betätigung der **Eingabetaste**.

3. Das Zertifkat wird durch OpenSSL erstellt und unter dem Dateinamen *ca.crt* gespeichert.

   WICHTIG: Verteilen Sie das Zertifikat *ca.crt* an die Webbrowser der Rechner, die die Webapplikation nutzen. Anhand dieses Zertifikats kann die Gültigkeit und das Vertrauen des eigenen Zertifkats im Gerät erfolgreich geprüft werden.

Erzeugen eines beliebigen Zertifikats

So erstellen Sie zunächst einen Schlüssel für das zu erstellende Zertifikat:

> **WICHTIG:** Der im folgenden Schritt zu erstellende Schlüssel wird nicht verschlüsselt. Lesen Sie ggf. in der Dokumentation von OpenSSL nach, um zu erfahren wie ein verschlüsselter Schlüssel erstellt werden kann!

1. Geben Sie folgenden Befehl in der Eingabeaufforderung ein und betätigen Sie anschließend die **Eingabetaste**:

```
openssl genrsa -out server.key 4096
```

2. Der Schlüssel wird durch OpenSSL erstellt und unter dem Dateinamen *server.key* gespeichert.

So erstellen Sie die Zertifikatsanforderung:

1. Geben Sie folgenden Befehl in der Eingabeaufforderung ein und betätigen Sie anschließend die **Eingabetaste**:

```
openssl req -new -key server.key -out server.csr
```

2. OpenSSL erfragt nun einige Daten, die in das Zertifikat integriert werden.

   Nachfolgend sind die verschiedenen Felder und eine exemplarische Eingabe aufgeführt:

Feld	Beispiel
Country Name (2 letter code)	DE
State or Province Name	NRW
Locality Name (eg, city)	Wilnsdorf
Organization Name (eg, company)	Guntermann & Drunck GmbH
Organizational Unit Name (eg, section)	
Common Name (eg, YOUR name)	192.168.0.10
Email Address	

> **WICHTIG:** Geben Sie die IP-Adresse des Geräts auf dem das Zertifikat installiert wird in der Zeile *Common Name* ein.

   Geben Sie die von Ihnen gewünschten Daten ein und bestätigen Sie jede Eingabe durch Betätigung der **Eingabetaste**.

3. Falls gewünscht, kann zusätzlich das *Challenge Password* festgelegt werden. Dieses ist bei Verlust des geheimen Schlüssels für einen Zertifikatwiderruf erforderlich.

4. Jetzt wird das Zertifikat erstellt und unter dem Dateinamen *server.csr* gespeichert.

X509-Zertifikat erstellen und signieren

1. Geben Sie folgenden Befehl in der Eingabeaufforderung ein und betätigen Sie anschließend die Eingabetaste:

```
openssl x509 -req -days 3650 -in server.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out server.crt
```

2. Das Zertifikat wird durch OpenSSL erstellt und unter dem Dateinamen *server.crt* gespeichert.

PEM-Datei erstellen

HINWEIS: Die *.pem*-Datei beinhaltet die folgenden drei Komponenten:

- Zertifikat des Servers
- Privater Schlüssel des Servers
- Zertifikat der Zertifizierungsstelle

Falls die drei Komponenten separat vorliegen, fügen Sie diese nacheinander im Feld *Klartext* ein, bevor Sie das im Gerät gespeicherte Zertifikat aktualisieren.

1. Geben Sie folgende(n) Befehl(e) in der Eingabeaufforderung ein und betätigen Sie anschließend die Eingabetaste:

   a. Linux

```
cat server.crt > gdcd.pem
cat server.key >> gdcd.pem
cat ca.crt >> gdcd.pem
```

   b. Windows

```
copy server.crt + server.key + ca.crt gdcd.pem
```

2. Durch die Kopieroperation(en) wird die Datei *gdcd.pem* erstellt. Diese enthält das erstellte Zertifikat und dessen Schlüssel sowie das Zertifikat der *Certificate Authority*.

Auswahl eines SSL-Zertifikats

Jedes G&D-Gerät mit integrierter Webapplikation wird ab Werk mit mindestens einem SSL-Zertifikat ausgestattet. Das Zertifikat erfüllt zwei Funktionen:

- Die Verbindung des Webbrowsers mit der Webapplikation kann über eine SSL-gesicherte Verbindung erfolgen. In diesem Fall erlaubt das SSL-Zertifikat dem Anwender , die Gegenseite zu authentifizieren.

  Weicht die IP-Adresse des Geräts von der im Zertifikat angegebenen IP-Adresse ab, wird eine Unstimmigkeit durch den Webbrowser gemeldet.

  TIPP: Importieren Sie ein eigenes Zertifikat, so dass die IP-Adresse des Geräts mit der im Zertifikat angegebenen übereinstimmt.

- Die Kommunikation verschiedener G&D-Geräte innerhalb eines KVM-Systems wird über die Zertifikate der Geräte abgesichert.

> **WICHTIG:** Nur wenn alle Geräte innerhalb eines KVM-Systems Zertifikate der identischen *Certificate Authority* (s. Seite 26) verwenden, können die Geräte miteinander kommunizieren.

So wählen Sie das zu verwendende SSL-Zertifikat:

> **HINWEIS:** Durch die Auswahl und Aktivierung eines *anderen* Zertifikates werden alle aktiven Sitzungen der Webapplikation beendet!

1. Klicken Sie in der Symbolleiste auf das Werkzeugsymbol.
2. Klicken Sie auf den Reiter **Zertifikat**.
3. Wählen Sie das zu verwendende Zertifikat aus:

G&D-Zertifikat #1:	Dieses Zertifikat ist bei *neuen* Geräten ab Werk aktiviert. **TIPP:** Ältere Geräte unterstützten *nicht* das **Zertifikat #1**.Verwenden Sie in diesem Fall **Zertifikat #2** oder **Eigenes Zertifikat**. innerhalb des KVM-Systems.
G&D-Zertifikat #2:	Dieses Zertifikat wird von allen G&D-Geräten mit integrierter Webapplikation unterstützt.
Eigenes Zertifikat:	Aktivieren Sie diese Option, wenn Sie ein gekauftes Zertifikat einer Zertifizierungsstelle oder ein selbsterstelltes Zertifikat verwenden möchten. Übertragen und aktivieren Sie anschließend das gewünschte Zertifikat: 1. Klicken Sie auf **Zertifikat aus Datei importieren** und wählen Sie die zu importierende .pem-Datei im Datei-Dialog aus. Alternativ kopieren Sie den Klartext des Zertifikats des Servers, den privaten Schlüssel des Servers sowie das Zertifikat der Zertifizierungsstelle in das Textfeld. 2. Klicken Sie auf **Upload und aktivieren**, um das importierte Zertifikat im Gerät zu speichern und zu aktivieren.

3. Klicken Sie auf **OK**, um den Dialog zu verlassen.

Durchführung eines Firmware-Updates

Die Firmware jedes Gerätes des KVM-Systems kann über die Webapplikation aktualisiert werden.

WICHTIG: Diese Funktion aktualisiert ausschließlich die Firmware des Gerätes, auf welchem die Webapplikation gestartet wurde!

So aktualisieren Sie die Firmware:

1. Öffnen Sie die Webapplikation des Gerätes, dessen Firmware Sie akualisieren möchten.
2. Klicken Sie in der Symbolleiste auf das Werkzeugsymbol.
3. Klicken Sie auf die Reiter **Werkzeuge** > **Firmware-Update**.
4. Geben Sie im Feld **Pfad** den Speicherort und den Namen der Update-Datei an.

   WICHTIG: Prüfen Sie anhand der Informationen der Felder *Gerät* und *Kommentar* des Dialogs, ob es sich um das gewünschte Gerät handelt.

   TIPP: Verwenden Sie die Datei-Schaltfläche, um den Speicherort und den Namen der Update-Datei über den Datei-Dialog auszuwählen.

5. Klicken Sie auf **Update ausführen**.
6. Klicken Sie auf **OK**, um den Dialog zu verlassen.

Wiederherstellung der Werkseinstellungen

Mit dieser Funktion kann die Werkseinstellung des Gerätes, auf welchem die Webapplikation betrieben wird, wiederhergestellt werden.

So stellen Sie die Werkseinstellungen wieder her:

WICHTIG: Alle vom Anwender veränderten Einstellungen werden zurückgesetzt.

1. Klicken Sie in der Symbolleiste auf das Werkzeugsymbol.
2. Klicken Sie auf die Reiter **Werkzeuge** > **Werkseinstellungen**.

   WICHTIG: Prüfen Sie anhand der Informationen der Felder *Gerät* und *Kommentar* des Dialogs, ob es sich um den gewünschten Matrixswitch handelt.

3. Deaktivieren Sie die Option **Netzwerkkonfiguration zurücksetzen**, falls Sie die Konfiguration der Netzwerkschnittstellen beibehalten möchten.
4. Klicken Sie auf **Werkseinstellungen**, um die aktuelle Konfiguration zurückzusetzen.

Neustart des Gerätes durchführen

Mit dieser Funktion starten Sie das Gerät neu. Vor dem Neustart werden Sie zur Bestätigung aufgefordert, um einen versehentlichen Neustart zu verhindern.

So führen Sie einen Neustart der Gerätes über die Webapplikation aus:

1. Klicken Sie im Strukturbaum auf **UserCenter**.
2. Klicken Sie mit der rechten Maustaste auf das gewünschte Gerät und anschließend auf **Neustart** im Kontextmenü.
3. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

TIPP: Alternativ können Sie den Neustart über das **Werkzeugsymbol** der Webapplikation durchführen. Klicken hierzu auf die Reiter **Werkzeuge > Neustart** und anschließend auf Neustart durchführen.

Netzwerkfunktionen der Geräte

Verschiedene Geräte innerhalb des KVM-Systems (z. B. *KVM-Extender* und *KVM-Matrixswitches*) verfügen über *separate* Netzwerkfunktionen.

Für jedes dieser Geräte innerhalb des KVM-Systems können u. a. folgende Funktionen konfigurieren:

- Authentifizierung gegenüber Verzeichnisdiensten (LDAP, Active Directory, RADIUS, TACACS+)
- Zeitsynchronisation über einen NTP-Server
- Versendung von Log-Meldungen an Syslog-Server
- Überwachung und Steuerung von Computern und Netzwerkgeräten über das *Simple Network Management Protocol* (s. Seite 52 ff.)

NTP-Server

Die Einstellung des Datums und der Uhrzeit eines Gerätes kann wahlweise automatisiert durch die Zeitsynchronisation mit einem NTP-Server (*Network Time Protocol*) oder manuell erfolgen.

Zeitsynchronisation mit einem NTP-Server

So ändern Sie die Einstellungen bezüglich der NTP-Zeitsynchronisation:

1. Klicken Sie im Strukturbaum auf **UserCenter**.
2. Klicken Sie mit der rechten Maustaste auf das zu konfigurierende Gerät und anschließend auf **Konfiguration** im Kontextmenü.
3. Klicken Sie auf den Reiter **Netzwerk**.

4. Klicken Sie auf den Reiter **NTP-Server** und erfassen Sie folgende Daten:

NTP-Zeitsynchro-nisation:	Durch Auswahl des entsprechenden Eintrags im Pull-Down-Menü können Sie die Zeitsynchronisation aus- und einschalten: ▪ **Deaktiviert** ▪ **Aktiviert**
NTP-Server 1:	Geben Sie die IP-Adresse eines Zeitservers ein.
NTP-Server 2:	Geben Sie *optional* die IP-Adresse eines zweiten Zeitservers ein.
Zeitzone:	Wählen Sie aus dem Pull-Down-Menü die Zeitzone Ihres Standorts aus.

5. Klicken Sie auf **OK**, um den Dialog zu verlassen.

Manuelle Einstellung von Uhrzeit und Datum

So stellen Sie die Uhrzeit und das Datum des Gerätes manuell ein:

1. Klicken Sie im Strukturbaum auf **UserCenter**.
2. Klicken Sie mit der rechten Maustaste auf das zu konfigurierende Gerät und anschließend auf **Konfiguration** im Kontextmenü.
3. Klicken Sie auf die Reiter **Netzwerk > NTP-Server**.
4. Deaktivieren Sie in diesem Dialog gegebenenfalls die Option **NTP-Zeitsynchronisation**, da andernfalls die manuelle Einstellung von Uhrzeit und Datum nicht möglich ist.
5. Geben Sie im Feld **Uhrzeit** die aktuelle Zeit im Format *hh:mm:ss* ein.
6. Geben Sie im Feld **Datum** das aktuelle Datum im Format *TT.MM.JJJJ* ein.

> **TIPP:** Klicken Sie auf **Lokales Datum übernehmen**, um das aktuelle Systemdatum des Computers, auf welchem die Webapplikation geöffnet wurde, in die Felder *Uhrzeit* und *Datum* zu übernehmen.

7. Klicken Sie auf **OK**.

Protokollierung von Syslog-Meldungen

Das Syslog-Protokoll wird zur Übermittlung von Log-Meldungen in Netzwerken verwendet. Die Log-Meldungen werden an einen Syslog-Server übermittelt, welcher die Log-Meldungen vieler Geräte im Rechnernetz protokolliert.

Im Syslog-Standard wurden u. a. acht verschiedene Schweregrade festgelegt, nach welchen die Log-Meldungen zu klassifizieren sind:

- **0:** Notfall
- **1:** Alarm
- **2:** Kritisch
- **3:** Fehler
- **4:** Warnung
- **5:** Notiz
- **6:** Info
- **7:** Debug

Über die Webapplikation können Sie die lokale Protokollierung oder den Versand von Syslog-Meldungen an bis zu zwei Syslog-Server konfigurieren.

Lokale Protokollierung der Syslog-Meldungen

So konfigurieren Sie die lokale Protokollierung von Syslog-Meldungen:

1. Klicken Sie im Strukturbaum auf **UserCenter**.
2. Klicken Sie mit der rechten Maustaste auf das zu konfigurierende Gerät und anschließend auf **Konfiguration** im Kontextmenü.
3. Klicken Sie auf den Reiter **Netzwerk**.
4. Klicken Sie auf den Reiter **Syslog** und erfassen Sie im Abschnitt **Syslog lokal** folgende Daten:

Syslog lokal:	Durch Auswahl des entsprechenden Eintrags im Pull-Down-Menü schalten Sie die lokale Protokollierung von Syslog-Meldungen aus oder ein: ▪ **Deaktiviert** ▪ **Aktiviert**
Log Level:	Wählen Sie in diesem Pull-Down-Menü aus, ab welchem Schweregrad eine Log-Meldung zu protokollieren ist. Der von Ihnen ausgewählte Schweregrad sowie alle niedrigeren Schweregrade werden protokolliert.

> Wählen Sie den Schweregrad *2 - Kritisch*, so werden für diesen, wie auch für die Schweregrade *1 - Alarm* und *0 - Notfall*, Meldungen protokolliert.

5. Klicken Sie auf **OK**, um den Dialog zu verlassen.

Versand von Syslog-Meldung an einen Server

So konfigurieren Sie den Versand von Syslog-Meldungen an einen Server:

1. Klicken Sie im Strukturbaum auf **UserCenter**.
2. Klicken Sie mit der rechten Maustaste auf das zu konfigurierende Gerät und anschließend auf **Konfiguration** im Kontextmenü.
3. Klicken Sie auf den Reiter **Netzwerk**.
4. Klicken Sie auf den Reiter **Syslog** und erfassen Sie folgende Daten im Abschnitt **Syslog-Server 1** oder **Syslog-Server 2**:

Syslog-Server:	Durch Auswahl des entsprechenden Eintrags im Pull-Down-Menü schalten Sie den Versand von Syslog-Meldungen an einen Server aus oder ein: ▪ **Deaktiviert** ▪ **Aktiviert**
Log Level:	Wählen Sie in diesem Pull-Down-Menü aus, ab welchem Schweregrad eine Log-Meldung zu protokollieren ist. Der von Ihnen ausgewählte Schweregrad sowie alle niedrigeren Schweregrade werden protokolliert.
Wählen Sie den Schweregrad *2 - Kritisch*, so werden für diesen, wie auch für die Schweregrade *1 - Alarm* und *0 - Notfall*, Meldungen protokolliert.	
IP-Adresse/ DNS-Name:	Geben Sie die IP-Adresse oder den Namen des Servers an, an welchen die Syslog-Meldungen zu senden sind.
Port:	Geben Sie den Port – üblicherweise 514 – an, auf welchem der Syslog-Server eingehende Meldungen annimmt.
Protokoll:	Wählen Sie das Protokoll – üblicherweise UDP – aus, auf welchem der Syslog-Server eingehende Meldungen annimmt: ▪ **TCP** ▪ **UDP**

5. Klicken Sie auf **OK**, um den Dialog zu verlassen.

Lokale Syslog-Meldung einsehen und speichern

Haben Sie die Protokollierung von lokalen Syslog-Meldungen aktiviert, können Sie diese Syslog-Meldung im Informationsdialog aufrufen und gegebenenfalls speichern.

So können Sie die lokalen Syslog-Meldungen einsehen und ggf. speichern:

1. Klicken Sie im Strukturbaum auf **System > Information**.
2. Klicken Sie mit der rechten Maustaste auf das zu konfigurierende Gerät und anschließend auf **Konfiguration** im Kontextmenü.
3. Doppelklicken Sie in der Hauptansicht auf **Syslog**.
4. Klicken Sie auf **SysLogs abrufen**.

   Die lokalen Syslog-Meldungen werden jetzt abgerufen und im Textfeld angezeigt.

   > **TIPP:** Klicken Sie gegebenenfalls auf **Speichern**, um die Meldungen in einer Textdatei zu speichern. Daraufhin erscheint ein Datei-Dialog, der Ihnen die Auswahl des Speicherortes und eines Dateinamens ermöglicht.
   >
   > Klicken Sie abschließend erneut auf **Speichern**.

5. Klicken Sie auf **OK**, um den Dialog zu verlassen.

Benutzerauthentifizierung mit Verzeichnisdiensten

In unternehmensinternen Netzwerken werden die Benutzerkonten häufig zentral durch einen Verzeichnisdienst verwaltet. Das Gerät kann auf einen solchen Verzeichnisdienst zugreifen und Benutzer gegen den Verzeichnisdienst authentisieren.

> **HINWEIS:** Scheitert die Authentifizierung des Benutzerkontos *Admin* durch den Verzeichnisdienst, wird das Benutzerkonto gegen die Datenbank des Gerätes authentifiziert!

Der Verzeichnisdienst wird ausschließlich zur Authentifizierung eines Benutzers verwendet. Die Vergabe von Rechten erfolgt durch die Datenbank des KVM-Systems. Hierbei wird zwischen folgenden Szenarien unterschieden:

- **Das Benutzerkonto existiert im Verzeichnisdienst und im KVM-System.**
  Der Benutzer kann sich mit dem im Verzeichnisdienst gespeicherten Passwort anmelden. Nach erfolgreicher Anmeldung werden dem Benutzer die Rechte des gleichnamigen Kontos im KVM-System zugewiesen.

  > **HINWEIS:** Das Passwort, mit dem sich der Benutzer erfolgreich angemeldet hat, wird in die Datenbank des KVM-Systems übernommen.

- **Das Benutzerkonto existiert im Verzeichnisdienst, aber nicht im KVM-System**
  Ein Benutzer, der erfolgreich gegen den Verzeichnisdienst authentifiziert wurde, aber kein gleichnamiges Konto in der Datenbank des KVM-Systems besitzt, wird mit den Rechten des Benutzers *RemoteAuth* ausgestattet.

  Ändern Sie ggf. die Rechte dieses speziellen Benutzerkontos, um die Berechtigung von Benutzern ohne eigenes Konto einzustellen.

  > **TIPP:** Deaktivieren Sie den Benutzer *RemoteAuth*, um die Anmeldung von Benutzern ohne eigenes Benutzerkonto im KVM-System zu verhindern.

- **Das Benutzerkonto existiert im KVM-System, aber nicht im Verzeichnisdienst**
  Ist der Verzeichnisdienst erreichbar, meldet dieser, dass das Benutzerkonto nicht existiert. Der Zugang zum KVM-System wird dem Benutzer verwehrt.

  Ist der Server nicht erreichbar, aber der Fallback-Mechanismus (s. Seite 39) aktiviert, kann sich der Benutzer mit dem im KVM-System gespeicherten Passwort anmelden.

  > **WICHTIG:** Um zu vermeiden, dass bei Ausfall der Verbindung zum Verzeichnisdienst die Anmeldung eines im Verzeichnisdienst gesperrten oder deaktivierten Benutzers möglich ist, beachten Sie folgende Sicherheitsregeln:
  >
  > - Wird im Verzeichnisdienst ein Benutzerkonto deaktiviert oder gelöscht, ist diese Aktion auch in der Benutzerdatenbank des KVM-Systems durchzuführen!
  > - Aktivieren Sie den Fallback-Mechanismus nur in begründeten Ausnahmefällen.

So konfigurieren Sie die Authentifizierung von Benutzerkonten:

> **HINWEIS:** Wird kein Verzeichnisdienst eingesetzt, werden die Benutzerkonten durch das Gerät verwaltet.

1. Klicken Sie im Strukturbaum auf **UserCenter**.
2. Klicken Sie mit der rechten Maustaste auf das zu konfigurierende Gerät und anschließend auf **Konfiguration** im Kontextmenü.
3. Klicken Sie auf den Reiter **Netzwerk > Authentifizierung** und erfassen Sie folgende Daten:

Auth. Server: Wählen Sie die Option **Lokal**, wenn die Benutzerverwaltung durch das KVM-System erfolgen soll.

Möchten Sie einen bestimmten Verzeichnisdienst nutzen, wählen Sie den entsprechenden Eintrag aus dem Pull-Down-Menü aus:

- **LDAP**
- **Active Directory**
- **Radius**
- **TACACS+**

> **TIPP:** Erfassen Sie nach der Auswahl eines Verzeichnisdienstes die Einstellungen des Verzeichnisdienst-Servers im Bereich *Servereinstellungen* der Dialogmaske.

Fallback: Aktivieren Sie diese Option, falls die lokale Benutzerverwaltung des KVM-Systems verwendet werden soll, wenn der Verzeichnisdienst temporär nicht verfügbar ist.

> **WICHTIG:** Um zu vermeiden, dass bei Ausfall der Verbindung zum Verzeichnisdienst die Anmeldung eines im Verzeichnisdienst gesperrten oder deaktivierten Benutzers möglich ist, beachten Sie folgende Sicherheitsregeln:
>
> - Wird im Verzeichnisdienst ein Benutzerkonto deaktiviert oder gelöscht, ist diese Aktion auch in der Benutzerdatenbank des KVM-Systems durchzuführen!
> - Aktivieren Sie den Fallback-Mechanismus nur in begründeten Ausnahmefällen.

4. Klicken Sie auf **OK**, um den Dialog zu verlassen.

Monitoring-Funktionen

In den gerätespezifischen Zweigen (beispielsweise *KVM-Matrixsysteme*) sowie in den Zweigen *KVM-Kombinationen* und *Kritische Geräte* des Strukturbaums können Sie die aktuellen Monitoring-Werte der Geräte des KVM-Systems einsehen.

Die verschiedenen Statusinformationen eines Gerätes können wahlweise als Einzelwerte oder in thematisch sortierten Monitoring-Gruppen angezeigt werden. Die folgende Abbildung zeigt beispielsweise den Einzelwert *Status* und drei verschiedene Monitoring-Gruppen:

	Name	Status	Gruppe #1	Gruppe #2	Gruppe #3
	Gerät #1	Online	Mehr...	Mehr...	Mehr...
	Gerät #2	Online	Mehr...	Mehr...	Mehr...
	Gerät #3	Online	Mehr...	Mehr...	Mehr...
	Gerät #4	Online	Mehr...	Mehr...	Mehr...
	Gerät #5	Online	Mehr...	Mehr...	Mehr...

Abbildung 2: Detailansicht einer exemplarischen Monitoring-Tabelle

Bei *Einzelwerten* (im obigen Beispiel der Wert *Status*) können Sie sofort erkennen, ob der Status einwandfrei (grüne Darstellung) oder auffällig (rote Darstellung) ist. Der ausgegebene Text in der Spalte gibt zusätzlich Auskunft über den aktuellen Zustand.

Die *Monitoring-Gruppen* erlauben Ihnen verschiedene Einzelwerte zu Gruppen zusammenzufassen. In der Tabelle wird Ihnen bei den Monitoring-Gruppen angezeigt, ob alle Werte einwandfrei (*grün*) oder mindestens ein Wert auffällig ist (*rot*).

Durch einen Klick auf den Pfeil innerhalb der Tabellenspalte, werden die verschiedenen Einzelwerte der Gruppe in einem separaten Fenster angezeigt.

Monitoring-Werte einsehen

HINWEIS: Eine Übersicht der möglichen Monitoring-Werte der verschiedenen Gerätearten finden Sie ab Seite 82.

Die Darstellung der Monitoring-Werte erfolgt in den unterschiedlichen Zweigen des Strukturbaums hauptsächlich durch Anwendung verschiedener Monitoring-Sets.

In einigen Zweigen (beispielsweise *Kritische Geräte*) wird von der Webapplikation eine andere Ansicht vorgegeben.

Auflistung der Werte durch Anwendung von Monitoring-Sets

Ein solches Monitoring-Set definiert die anzuzeigenden Einzelwerte und Gruppen.

In den Tabellenzellen der *Einzelwerte* können Sie sofort erkennen, ob der Status einwandfrei oder auffällig ist und diesen ablesen.

Die *Monitoring-Gruppen* hingegen fassen verschiedene Einzelwerte zu Gruppen zusammen. In der Tabellenzelle einer Monitoring-Gruppe wird angezeigt, ob alle Werte einwandfrei (grün) oder mindestens ein Wert auffällig ist (rot).

Ein Klick auf den Pfeil innerhalb der Tabellenspalte öffnet ein Fenster mit Detailinformationen zu den Einzelwerten der Gruppe.

TIPP: Detaillierte Informationen zu Monitoring-Gruppen und -Sets finden Sie auf den folgenden Seiten dieses Kapitels.

Auflistung der Einzelwerte kritischer Geräte

Liegt bei einem Gerät mindestens ein auffälliger Wert vor, erfolgt die zusätzliche Auflistung des Gerätes im Zweig Kritische Geräte. Hier werden ausschließlich die auffälligen (roten) Werte in der Tabelle angezeigt, um einen schnellen Überblick über die kritischen Monitoring-Werte zu ermöglichen.

HINWEIS: Um eine schnelle Übersicht über die auffälligen Werte zu ermöglichen, wird hier auf die Anwendung von Monitoring-Sets verzichtet.

Monitoring-Werte deaktivieren

Sie können beliebige Monitoring-Werte deaktivieren. Diese Werte werden daraufhin nicht mehr in der Webapplikation angezeigt.

WICHTIG: Zu deaktivierten Monitoring-Werte erscheinen keine Warnungen in der Web-Applikation und es werden keine SNMP-Traps hierzu versendet!

So (de)aktivieren Sie Monitoring-Werte:

1. Klicken Sie im Strukturbaum auf **UserCenter**.
2. Klicken Sie mit der rechten Maustaste auf das zu konfigurierende Gerät und anschließend auf **Konfiguration** im Kontextmenü.

3. Klicken Sie auf den Reiter **Monitoring**.

   Der Dialog besteht aus zwei Tabellen, in welchen die Monitoring-Werte des KVM-Systems aufgelistet werden:

Aktiviert:	Auflistung der aktivierten Monitoring-Werte.
Deaktiviert:	Auflistung der deaktivierten Monitoring-Werten.

   Für eine bessere Übersicht werden die Werte – sowohl in der linken, als auch in der rechten Spalte – gruppiert dargestellt.

4. Markieren Sie den Monitoring-Wert, welchen Sie (de)aktivieren möchten.

5. Klicken Sie auf (*Pfeil rechts*), um den Monitoring-Wert zu deaktivieren oder auf (*Pfeil links*), um diesen zu aktivieren.

6. Klicken Sie auf **OK**, um die geänderten Einstellungen zu speichern.

Erweiterte Funktionen zur Verwaltung der kritischen Geräte

Wie bereits erwähnt, werden im Zweig *Kritische Geräte* die Geräte aufgelistet, bei welchen mindestens ein Wert außerhalb des Sollbereichs liegt.

> **HINWEIS:** Für jede Geräteklasse innerhalb des KVM-Systems (z. B. *KVM-Matrixsysteme*) wird ein Unterzweig eingeblendet.

Hinweis auf den kritischen Status von Geräten

Falls ein Wert außerhalb des Sollbereichs liegt, wird der Zweig rot markiert und unterhalb der Hauptansicht werden Sie durch einen blinkenden Hinweis auf den Sachverhalt aufmerksam gemacht.

> **TIPP:** Erscheint ein blinkender Hinweis am unteren Rand der Hauptansicht, können Sie durch Betätigung der Tastenkombination **Strg+Space** sofort den Zweig *Kritische Geräte* öffnen.
>
> Klicken Sie mit dem Mauszeiger auf den blinkenden Hinweis, um die Auflistung der Unstimmigkeiten in einem separaten Fenster anzuzeigen.

Auflistung der kritischen Geräte einsehen

So zeigen Sie die Auflistung der kritischen Geräte an:

1. Klicken Sie im Strukturbaum auf die Ordner **Systemüberwachung > Kritische Geräte**.

   In der Hauptansicht werden die betroffenen Geräte aufgelistet. Die kritischen Werte werden in der Tabellenansicht angezeigt.

   > **TIPP:** Klicken Sie auf einen Unterzweig des Ordners, um die Auflistung der Geräte auf eine bestimmte Geräteklasse einzugrenzen

Meldungen eines kritischen Gerätes als gesehen markieren

Viele Meldungen erfordern ein sofortiges Handeln des Administrators. Andere Meldungen hingegen (beispielsweise der Ausfall der redundanten Stromversorgung) weisen auf möglicherweise unkritische Sachverhalte hin.

In einem solchen Fall, können alle auffälligen Werte eines Gerätes als gesehen markiert werden. Hierdurch erreichen Sie folgendes Programmverhalten:

- Ein Gerät, dessen auffällige Werte als gesehen markiert wurden, führt nicht zu einer blinkenden Statuszeile.
- Die Darstellung der „gesehenen“ Werte erfolgt in allen Tabellenzellen, Infodialogen und Monitoring-Fenstern mit gelber Farbhinterlegung.
- Wenn in einer Monitoring-Gruppe als gelesen markierte kritische Werte enthalten sind, wird – wie üblich – in der Tabellenspalte *Fehler* angezeigt. Zusätzlich wird die Tabellenzelle gelb hinterlegt.

HINWEIS: Die Markierung bezieht sich ausschließlich auf, zum Zeitpunkt der Ausführung der Funktion, auffällige Werte. Wird ein weiterer Monitoring-Wert eines solchen Gerätes auffällig, weist die Webapplikation hierauf hin.

So markieren Sie die Monitoring-Meldungen eines Gerätes als gelesen:

1. Klicken Sie im Strukturbaum auf die Ordner **Systemüberwachung > Kritische Geräte**.
2. Klicken Sie mit der rechten Maustaste aus das gewünschte Gerät und anschließend auf den Eintrag **Gesehen** des Kontextmenüs.

Verwaltung der Monitoring-Gruppen

WICHTIG: Die angelegten Monitoring-Gruppen sind ausschließlich in dem Zweig des Strukturbaums verfügbar, in welchem sie angelegt wurden.

Wurde eine Monitoring-Gruppe innerhalb eines gerätespezifischen Zweiges angelegt, ist diese im Zweig *KVM-Kombinationen* nicht verfügbar!

In der Webapplikation *Config Panel* sind einige Monitoring-Gruppen bereits vorkonfiguriert. Diese Gruppen können weder editiert noch gelöscht werden. Das Duplizieren und die anschließende individuelle Anpassung der Gruppe an Ihre Wünsche ist möglich.

Die vorkonfigurierten bzw. von Ihnen erstellten Gruppen werden – sofern sie im angewendeten Monitoring-Set enthalten sind (s. Seite 50 ff.) – in der Monitoring-Tabelle angezeigt:

	Name	Status	Gruppe #1	Gruppe #2	Gruppe #3
	Gerät #1	Online	Mehr...	Mehr...	Mehr...
	Gerät #2	Online	Mehr...	Mehr...	Mehr...
	Gerät #3	Online	Mehr...	Mehr...	Mehr...
	Gerät #4	Online	Mehr...	Mehr...	Mehr...
	Gerät #5	Online	Mehr...	Mehr...	Mehr...

Abbildung 3: Status der Werte der Monitoring-Gruppe »Gruppe #1« verschiedener Geräte

TIPP: Aufgrund der hohen Anzahl an Einzelwerten ist es empfehlenswert, die wichtigsten Werte als Einzelwerte und die übrigen in thematischen Gruppen gegliedert anzuzeigen.

Sie erreichen so den schnellen Überblick und eine platzsparende Darstellung.

Hinzufügen einer Monitoring-Gruppe

So legen Sie eine neue Monitoring-Gruppe an:

1. Klicken Sie im Strukturbaum mit der rechten Maustaste auf die oberste Ebene eines gerätespezifischen Zweiges (beispielsweise *UserCenter*) oder auf den Zweig *KVM-Kombinationen*.
2. Klicken Sie auf den Eintrag **Monitoring-Gruppen** im Kontextmenü.
3. Klicken Sie auf **Hinzufügen**.
4. Erfassen Sie den Namen und ggf. einen optionalen Kommentar der neuen Gruppe.
5. Klicken Sie auf **OK**, um die neue Gruppe anzulegen.

Namen und/oder Kommentar einer Monitoring-Gruppe ändern

So ändern Sie den Namen und/oder Kommentar einer Monitoring-Gruppe:

1. Klicken Sie im Strukturbaum mit der rechten Maustaste auf die oberste Ebene eines gerätespezifischen Zweiges (beispielsweise *UserCenter*) oder auf den Zweig *KVM-Kombinationen*.
2. Klicken Sie auf den Eintrag **Monitoring-Gruppen** im Kontextmenü.
3. Wählen Sie die zu editierende Gruppe und klicken Sie auf **Ändern**.
4. Ändern Sie den Namen und/oder den optionalen Kommentar der Gruppe.
5. Klicken Sie auf **OK**, um die geänderten Einstellungen zu speichern.

Mitglieder einer Monitoring-Gruppe festlegen

So legen Sie die Mitglieder einer Monitoring-Gruppe fest:

1. Klicken Sie im Strukturbaum mit der rechten Maustaste auf die oberste Ebene eines gerätespezifischen Zweiges (beispielsweise *UserCenter*) oder auf den Zweig *KVM-Kombinationen*.
2. Klicken Sie auf den Eintrag **Monitoring-Gruppen** im Kontextmenü.
3. Wählen Sie die zu editierende Gruppe und klicken Sie auf **Ändern**.
4. Klicken Sie auf die Registerkarte **Mitglieder**.

   Hier haben Sie die Möglichkeit, Mitglieder der Monitoring-Gruppe hinzuzufügen oder aus dieser zu entfernen.

   Der Dialog besteht aus zwei Tabellen, in welchen die Monitoring-Werte des KVM-Systems aufgelistet werden:

Nicht zugeordnet:	Anzeige von Monitoring-Werten, die dieser Gruppe *nicht* zugeordnet sind.
Zugeordnete Gruppenmitglieder:	Anzeige von Monitoring-Werten, die dieser Gruppe zugeordnet sind.

5. Markieren Sie den Monitoring-Wert, welchen Sie der Gruppe hinzufügen oder aus dieser entfernen möchten.
6. Klicken Sie auf (*Pfeil rechts*), um den Monitoring-Wert der Gruppe hinzuzufügen oder auf (*Pfeil links*), um diesen aus der Mitgliederliste zu entfernen.
7. Klicken Sie auf **OK**, um die geänderten Einstellungen zu speichern.

Duplizieren einer Monitoring-Gruppe

In vielen gerätespezifischen Zweigen, wie auch im Zweig *KVM-Kombinationen*, sind einige Gruppen vorkonfiguriert. Diese Gruppen werden in der Auflistung in hellgrauer Schrift dargestellt.

WICHTIG: Das Bearbeiten und Löschen dieser Gruppen ist *nicht* möglich.

Möchten Sie eine neue Gruppe auf Basis einer bereits bestehenden Gruppe erstellen, können Sie die bestehende Gruppe zunächst duplizieren und das Duplikat anschließend bearbeiten.

So duplizieren Sie eine Monitoring-Gruppe:

1. Klicken Sie im Strukturbaum mit der rechten Maustaste auf die oberste Ebene eines gerätespezifischen Zweiges (beispielsweise *UserCenter*) oder auf den Zweig *KVM-Kombinationen*.

1. Klicken Sie auf den Eintrag **Monitoring-Gruppen** im Kontextmenü.
2. Wählen Sie die zu duplizierende Gruppe und klicken Sie auf **Ändern**.

3. Erfassen Sie den Namen der neuen Gruppe und ggf. einen optionalen Kommentar der Gruppe.
4. Klicken Sie auf **Duplizieren**, um die bestehende Gruppe zu duplizieren.
5. Bearbeiten Sie die neue Gruppe, wie auf den vorangegangenen Seite beschrieben oder klicken Sie auf **Schließen**, um das Fenster zu schließen.

Löschen einer Monitoring-Gruppe

In vielen gerätespezifischen Zweigen, wie auch im Zweig *KVM-Kombinationen*, sind einige Gruppen vorkonfiguriert. Diese Gruppen werden in der Auflistung in hellgrauer Schrift dargestellt.

WICHTIG: Das Bearbeiten und Löschen dieser Gruppen ist *nicht* möglich.

So löschen Sie eine Monitoring-Gruppe:

1. Klicken Sie im Strukturbaum mit der rechten Maustaste auf die oberste Ebene eines gerätespezifischen Zweiges (beispielsweise *UserCenter*) oder auf den Zweig *KVM-Kombinationen*.
2. Klicken Sie auf den Eintrag **Monitoring-Gruppen** im Kontextmenü.
3. Wählen Sie die zu löschende Gruppe und klicken Sie auf **Löschen**.
4. Bestätigen Sie die erscheinende Sicherheitsabfrage durch Klick auf **Ja** oder brechen Sie den Vorgang durch Klick auf **Nein** ab.
5. Klicken Sie auf **Schließen**, um die geänderten Einstellungen zu speichern.

Verwaltung der Monitoring-Sets

Ein Monitoring-Set definiert die anzuzeigenden Einzelwerte und Gruppen eines Unterordners des Zweiges *KVM-Kombinationen* oder eines gerätespezifischen Zweiges:

	Name	Status	Gruppe #1	Gruppe #2	Gruppe #3
	Gerät #1	Online	Mehr...	Mehr...	Mehr...
	Gerät #2	Online	Mehr...	Mehr...	Mehr...
	Gerät #3	Online	Mehr...	Mehr...	Mehr...
	Gerät #4	Online	Mehr...	Mehr...	Mehr...
	Gerät #5	Online	Mehr...	Mehr...	Mehr...

Abbildung 4: Status des Einzelwertes *Status* und dreier Gruppen eines Monitoring-Sets

In der Webapplikation *Config Panel* sind einige Monitoring-Sets bereits vorkonfiguriert. Diese Sets können weder editiert noch gelöscht werden. Das Duplizieren und die anschließende individuelle Anpassung des Sets an Ihre Wünsche ist möglich.

Alternativ ist das Erstellen und die anschließende Konfiguration einer neuen Gruppe möglich.

WICHTIG: Die angelegten Monitoring-Sets sind ausschließlich in dem Zweig des Strukturbaums verfügbar, in welchem Sie angelegt wurden.

Wurde ein Monitoring-Set beispielsweise innerhalb eines gerätespezifischen Zweiges angelegt, ist dieses im Zweig *KVM-Kombinationen* nicht verfügbar!

Hinzufügen eines Monitoring-Sets

So legen Sie ein neues Monitoring-Set an:

1. Klicken Sie im Strukturbaum mit der rechten Maustaste auf die oberste Ebene eines gerätespezifischen Zweiges (beispielsweise *UserCenter*) oder auf den Zweig *KVM-Kombinationen*.
2. Klicken Sie auf den Eintrag **Monitoring-Set** im Kontextmenü.
3. Klicken Sie auf **Hinzufügen**.
4. Erfassen Sie den Namen und ggf. einen optionalen Kommentar des neuen Sets.
5. Klicken Sie auf **OK**, um das neue Set anzulegen.

Namen und/oder Kommentar eines Monitoring-Sets ändern

So ändern Sie den Namen und/oder Kommentar eines Monitoring-Sets:

1. Klicken Sie im Strukturbaum mit der rechten Maustaste auf die oberste Ebene eines gerätespezifischen Zweiges (beispielsweise *UserCenter*) oder auf den Zweig *KVM-Kombinationen*.
2. Klicken Sie auf den Eintrag **Monitoring-Sets** im Kontextmenü.
3. Wählen Sie das zu editierende Set und klicken Sie auf **Ändern**.
4. Ändern Sie den Namen und/oder den optionalen Kommentar des Sets.
5. Klicken Sie auf **OK**, um die geänderten Einstellungen zu speichern.

Mitglieder eines Monitoring-Sets festlegen

WICHTIG: Legen Sie die im Monitoring-Set zu berücksichtigenden Monitoring-Gruppen (s. Seite 44 ff.) unbedingt *vor* dem Erstellen eines Sets an!

So legen Sie die Mitglieder eines Monitoring-Sets fest:

1. Klicken Sie im Strukturbaum mit der rechten Maustaste auf die oberste Ebene eines gerätespezifischen Zweiges (beispielsweise *UserCenter*) oder auf den Zweig *KVM-Kombinationen*.
2. Klicken Sie auf den Eintrag **Monitoring-Sets** im Kontextmenü.
3. Wählen Sie das zu editierende Set und klicken Sie auf **Ändern**.
4. Klicken Sie auf die Registerkarte **Mitglieder**.

   Hier haben Sie die Möglichkeit, dem Monitoring-Set Mitglieder hinzuzufügen oder solche aus diesem zu entfernen.

   Der Dialog besteht aus zwei Tabellen, in welchen die Monitoring-Werte des KVM-Systems aufgelistet werden. Die Werte werden in die Kategorien *Einzelwerte* und *Gruppen (Spalten)* unterteilt.

   HINWEIS: Klicken Sie auf **[-]** im Titel einer Kategorie, um die Inhalte dieser Kategorie auszublenden. Ein Klick auf **[+]** blendet die Inhalte ein.

   Die verschiedenen Werte werden entweder in der linken oder rechten Tabelle aufgelistet:

Nicht zugeordnet:	Anzeige von Einzelwerten und Monitoring-Gruppen, die diesem Set *nicht* zugeordnet sind.
Zugeordnete Gruppenmitglieder:	Anzeige von Einzelwerten und Monitoring-Gruppen, die diesem Set zugeordnet sind.

5. Markieren Sie den Einzelwert oder die Monitoring-Gruppe, den bzw. die Sie dem Set hinzufügen oder aus diesem entfernen möchten.

6. Klicken Sie auf (*Pfeil rechts*), um das ausgewählte Element dem Set hinzuzufügen oder auf (*Pfeil links*), um diesen aus dem Set zu entfernen.
7. Klicken Sie auf **OK**, um die geänderten Einstellungen zu speichern.

Auswahl eines Monitoring-Sets in der Ordner-Konfiguration

Nach der Erstellung eines Monitoring-Sets können Sie dieses in der Konfiguration eines (oder mehrer) Ordner des Strukturbaums aktivieren.

So aktivieren Sie ein Monitoring-Set:

1. Klicken Sie im Strukturbaum mit der rechten Maustaste auf die oberste Ebene eines gerätespezifischen Zweiges (beispielsweise *UserCenter*) oder auf den Zweig *KVM-Kombinationen*.
2. Klicken Sie auf den Eintrag **Konfiguration** im Kontextmenü.
3. Wählen Sie im Feld **Monitoring-Set** das gewünschte Set aus.

   WICHTIG: Die angelegten Monitoring-Sets sind ausschließlich in dem Zweig des Strukturbaums verfügbar, in welchem Sie angelegt wurden.

   Wurde ein Monitoring-Set beispielsweise im Zweig *KVM-Matrixsysteme* angelegt, ist dieses im Zweig *KVM-Kombinationen* nicht verfügbar!

4. Klicken Sie auf **OK**, um das ausgewählte Set zu aktivieren.

Duplizieren eines Monitoring-Sets

In vielen gerätespezifischen Zweigen, wie auch im Zweig *KVM-Kombinationen*, sind einige Sets vorkonfiguriert. Diese Sets werden in der Auflistung in hellgrauer Schrift dargestellt.

WICHTIG: Das Bearbeiten und Löschen dieser Sets ist *nicht* möglich.

Möchten Sie ein neues Set auf Basis eines bereits bestehenden Sets erstellen, können Sie das bestehende Set zunächst duplizieren und das Duplikat anschließend bearbeiten.

So duplizieren Sie ein Monitoring-Set:

1. Klicken Sie im Strukturbaum mit der rechten Maustaste auf die oberste Ebene eines gerätespezifischen Zweiges (beispielsweise *UserCenter*) oder auf den Zweig *KVM-Kombinationen*.
2. Klicken Sie auf den Eintrag **Monitoring-Sets** im Kontextmenü.
3. Wählen Sie das zu duplizierende Set und klicken Sie auf **Ändern**.
4. Erfassen Sie den Namen des neuen Sets und ggf. einen optionalen Kommentar der Gruppe.

5. Klicken Sie auf Duplizieren, um das bestehende Set zu duplizieren.
6. Bearbeiten Sie das neue Set, wie auf den vorangegangenen Seite beschrieben oder klicken Sie auf **Schließen**, um das Fenster zu schließen.

Löschen eines Monitoring-Sets

In vielen gerätespezifischen Zweigen, wie auch im Zweig *KVM-Kombinationen*, sind einige Sets vorkonfiguriert. Diese Sets werden in der Auflistung in hellgrauer Schrift dargestellt.

> **WICHTIG:** Das Bearbeiten und Löschen dieser Sets ist *nicht* möglich.

So löschen Sie ein Monitoring-Set:

1. Klicken Sie im Strukturbaum mit der rechten Maustaste auf die oberste Ebene eines gerätespezifischen Zweiges (beispielsweise *UserCenter*) oder auf den Zweig *KVM-Kombinationen*.
2. Klicken Sie auf den Eintrag **Monitoring-Sets** im Kontextmenü.
3. Wählen Sie die zu löschende Set und klicken Sie auf **Löschen**.
4. Bestätigen Sie die erscheinende Sicherheitsabfrage durch Klick auf **Ja** oder brechen Sie den Vorgang durch Klick auf **Nein** ab.
5. Klicken Sie auf **Schließen**, um die geänderten Einstellungen zu speichern.

Geräteüberwachung via SNMP

Das *Simple Network Management Protocol* (SNMP) wird zur Überwachung und Steuerung von Computern und Netzwerkgeräten verwendet.

Praktischer Einsatz des SNMP-Protokolls

Zur Überwachung und Steuerung von Computern und Netzwerkgeräten wird in einem Netzwerk ein *Network Management System* (NMS) betrieben, das die Daten der zu überwachenden Geräte von deren *Agents* anfordert und sammelt.

HINWEIS: Ein *Agent* ist ein Programm, das auf dem überwachten Gerät läuft und dessen Status ermittelt. Über SNMP werden die ermittelten Daten an das *Network Management System* übermittelt.

Erkennt ein *Agent* ein schwerwiegendes Ereignis auf dem Gerät, kann er selbstständig ein *Trap*-Paket an das *Network Management System* senden. So wird sichergestellt, dass der Administrator kurzfristig über das Ereignis informiert wird.

Konfiguration des SNMP-Agents

So konfigurieren Sie den SNMP-Agent:

1. Klicken Sie im Strukturbaum auf **UserCenter**.
2. Klicken Sie mit der rechten Maustaste auf das zu konfigurierende Gerät und anschließend auf **Konfiguration** im Kontextmenü.
3. Klicken Sie auf die Reiter **Netzwerk > SNMP Agent**.
4. Erfassen Sie im Abschnitt *Global* folgende Daten:

Aktiviert:	Durch Auswahl des entsprechenden Eintrags schalten Sie den SNMP-Agent aus (**Aus**) oder ein (**Aktiviert**).
Protokoll:	Wählen Sie das Protokoll (**TCP** oder **UDP**) – üblicherweise UDP – aus, über welches die SNMP-Pakete übertragen werden sollen.
Port:	Geben Sie den Port – üblicherweise 161 – an, auf welchem *eingehende* SNMP-Pakete akzeptiert werden.

SysContact:	Geben Sie die Kontaktdaten (beispielweise Durchwahl oder E-Mail-Adresse) des Administrators ein.
SysName:	Geben Sie den Namen des Gerätes ein.
SysLocation:	Geben Sie den Standort des Gerätes ein.

5. Möchten Sie Pakete der Protokollversion **SNMPv2c** verarbeiten, erfassen Sie im gleichnamigen Abschnitt die auf der folgenden Seite aufgeführten Daten.

Access:	Aktivieren Sie den lesenden Zugriff (**View**) oder verweigern Sie den Zugriff (**No**) über das *SNMPv2c*-Protokoll.
Source:	Geben Sie die IP-Adresse oder den Adressraum der Adressen eingehender SNMP-Pakete ein. **Beispiele:** ▪ **192.168.150.187:** nur die IP-Adresse 192.168.150.187 ▪ **192.168.150.0/24:** IP-Adressen des Raums 192.168.150.x ▪ **192.168.0.0/16:** IP-Adressen des Raums 192.168.x.x ▪ **192.0.0.0/8:** IP-Adressen des Raums 192.x.x.x
Read-only community:	Geben Sie die Bezeichnung der *Community* ein, welche auch im *Network Management System* gewählt wurde.

WICHTIG: Das Passwort (*Community*) der Pakete der Protokollversion *SNMPv2c* wird unverschlüsselt übertragen und kann daher leicht abgehört werden!

Verwenden Sie ggf. die Protokollversion *SNMPv3* (s. u.) und einen hohen *Security-Level*, um eine sichere Übertragung der Daten zu erreichen.

6. Möchten Sie Pakete der Protokollversion **SNMPv3** verarbeiten, erfassen Sie im gleichnamigen Abschnitt folgende Daten:

Access:	Aktivieren Sie den lesenden Zugriff (**View**) oder verweigern Sie den Zugriff (**No**) über das *SNMPv3*-Protokoll.
Benutzername:	Geben Sie den Benutzernamen für die Kommunikation mit dem *Network Management System* an.
Authentifizierungs-Protokoll	Wählen Sie das im *Network Management System* aktivierte Authentifizierungs-Protokoll (**MD5** oder **SHA**) aus.
Authentifizierungs-Passwort	Geben Sie das Authentifizierungs-Passwort für die Kommunikation mit dem *Network Management System* an.
Security-Level	Wählen Sie zwischen einer der folgenden Optionen: ▪ **NoAuthNoPriv:** Benutzer-Authentifizierung und *Privacy*-Protokoll deaktiviert ▪ **AuthNoPriv:** Benutzer-Authentifizierung aktiviert, *Privacy*-Protokoll deaktiviert ▪ **AuthPriv:** Benutzer-Authentifizierung und *Privacy*-Protokoll aktiviert

Privacy-Protokoll:	Wählen Sie das im *Network Management System* aktivierte Privacy-Protokoll (**DES** oder **AES**) aus.
Privacy-Passwort:	Geben Sie das Privacy-Passwort für die gesicherte Kommunikation mit dem *Network Management System* an.
Engine-ID-Methode:	Wählen Sie, nach welcher Methode die **SnmpEngineID** vergeben werden soll: ▪ **Random:** Die *SnmpEngineID* wird bei jedem Neustart des Gerätes neu vergeben. ▪ **Fix:** Die *SnmpEngineID* entspricht der MAC-Adresse der ersten Netzwerkschnittstelle des Gerätes. ▪ **User:** Der im Feld *Engine-ID* eingetragene String wird als *SnmpEngineID* verwendet.
Engine-ID	Bei Verwendung der *Engine-ID-Methode* **User** geben Sie hier den String ein, der als *Engine-ID* verwendet wird.

7. Klicken Sie auf **OK**, um die Daten zu speichern und den Dialog zu verlassen.

Konfiguration von SNMP-Traps

So fügen Sie einen neuen Trap hinzu oder bearbeiten einen vorhandenen Trap:

1. Klicken Sie im Strukturbaum auf **UserCenter**.
2. Klicken Sie mit der rechten Maustaste auf das zu konfigurierende Gerät und anschließend auf **Konfiguration** im Kontextmenü.
3. Klicken Sie auf die Reiter **Netzwerk > SNMP-Trap**.
4. Klicken Sie auf **Hinzufügen** bzw. auf **Bearbeiten**.
5. Erfassen Sie im Abschnitt **Global** folgende Daten:

Server:	Geben Sie die IP-Adresse des *Network Management Servers* ein.
Protokoll:	Wählen Sie das Protokoll (**TCP** oder **UDP**) – üblicherweise UDP – aus, über welches die SNMP-Pakete übertragen werden sollen.
Port:	Geben Sie den Port – üblicherweise 162 – an, auf welchem *ausgehende* SNMP-Pakete übertragen werden.

Versuche:	Geben Sie die Anzahl der Versand-Wiederholungen eines *SNMP Informs* an. **HINWEIS:** Eine Eingabe ist nur möglich, wenn im Feld *Notification type* die Option *Inform* gewählt wurde.

Timeout:	Geben Sie das Timeout (in Sekunden) ein, nach welchem die erneute Aussendung eines *SNMP Informs* erfolgt, wenn keine Bestätigung erfolgt.
	HINWEIS: Eine Eingabe ist nur möglich, wenn im Feld *Notification type* die Option *Inform* gewählt wurde.
Log-Level:	Wählen Sie den Schweregrad eines Ereignisses aus, ab welchem ein SNMP-Trap zu versenden ist. Der von Ihnen ausgewählte Schweregrad sowie alle niedrigeren Schweregrade werden protokolliert.
	HINWEIS: Wählen Sie den Schweregrad *2 - Kritisch*, so werden bei Ereignissen dieses, wie auch der Schweregrade *1 - Alarm* und *0 - Notfall*, SNMP-Traps ausgesendet.
Version:	Wählen Sie, ob die Traps gemäß der Protokollversion *SNMPv2c* (**v2c**) oder *SNMPv3* (**v3**) erstellt und versendet werden.
Notification type:	Wählen Sie, ob die Ereignisse als *Trap*- oder *Inform*-Paket versendet werden.
	HINWEIS: *Inform*-Pakete erfordern eine Bestätigung des *Network Management Systems*. Liegt diese nicht vor, wird die Übertragung wiederholt.

6. Haben Sie sich im letzten Schritt für die Protokollversion **SNMPv2c** entschieden, erfassen Sie im gleichnamigen Abschnitt die Bezeichnung der *Community*, welche auch im *Network Management System* gewählt wurde.

> **WICHTIG:** Das Passwort (*Community*) der Pakete der Protokollversion *SNMPv2c* wird unverschlüsselt übertragen und kann daher leicht abgehört werden!
>
> Verwenden Sie ggf. die Protokollversion *SNMPv3* (s. u.) und einen hohen *Security-Level*, um eine sichere Übertragung der Daten zu erreichen.

7. Haben Sie sich in Schritt 5. für die Protokollversion **SNMPv3** entschieden, erfassen Sie im gleichnamigen Abschnitt folgende Daten:

Benutzername:	Geben Sie den Benutzernamen für die Kommunikation mit dem *Network Management System* an.
Authentifizierungs-Protokoll	Wählen Sie das im *Network Management System* aktivierte Authentifizierungs-Protokoll (**MD5** oder **SHA**) aus.
Authentifizierungs-Passwort	Geben Sie das Authentifizierungs-Passwort für die Kommunikation mit dem *Network Management System* an.

Security-Level	Wählen Sie zwischen einer der folgenden Optionen: ▪ **NoAuthNoPriv:** Benutzer-Authentifizierung und *Privacy*-Protokoll deaktiviert ▪ **AuthNoPriv:** Benutzer-Authentifizierung aktiviert, *Privacy*-Protokoll deaktiviert ▪ **AuthPriv:** Benutzer-Authentifizierung und *Privacy*-Protokoll aktiviert
Privacy-Protokoll:	Wählen Sie das im *Network Management System* aktivierte Privacy-Protokoll (**DES** oder **AES**) aus.
Privacy-Passwort:	Geben Sie das Privacy-Passwort für die gesicherte Kommunikation mit dem *Network Management System* an.
Engine-ID:	Geben Sie eine *Engine-ID* ein, die den SNMP-Agent eindeutig im Netzwerk identifiziert.

8. Klicken Sie auf **OK**, um die Daten zu speichern und den Dialog zu verlassen.

So löschen Sie einen vorhandenen Trap:

1. Klicken Sie im Strukturbaum auf **UserCenter**.
2. Klicken Sie mit der rechten Maustaste auf das zu konfigurierende Gerät und anschließend auf **Konfiguration** im Kontextmenü.
3. Klicken Sie auf die Reiter **Netzwerk > SNMP-Trap**.
4. Klicken Sie in der Zeile des zu löschenden Receivers auf **Löschen**.
5. Klicken Sie auf **OK**, um die Daten zu speichern und den Dialog zu verlassen.

So generieren Sie ein Test-Event:

1. Klicken Sie im Strukturbaum auf **UserCenter**.
2. Klicken Sie mit der rechten Maustaste auf das zu konfigurierende Gerät und anschließend auf **Konfiguration** im Kontextmenü.
3. Klicken Sie auf die Reiter **Netzwerk > SNMP-Trap**.
4. Klicken Sie auf **Test-Event generieren**.
5. Klicken Sie auf **OK**, um die Daten zu speichern und den Dialog zu verlassen.

HINWEIS: Bei korrekter Konfiguration wird die *Trap*-Meldung innerhalb Ihres *Network Management Systems* angezegt.

Logbuch

Im *Logbuch* eines Gerätes des KVM-Systems können Sie beliebige Informationen erfassen.

> **TIPP:** Notieren Sie beispielsweise geplante Änderungen an der Konfiguration des Gerätes und weisen Sie dem Eintrag den Status »offen« zu.
>
> Nach der Durchführung der Änderungen weisen Sie dem Logbuch-Eintrag den Status »erledigt« zu. Der Zeitpunkt der Erledigung kann später im Logbuch „nachschlagen" werden.

Die Logbücher der verschiedenen Geräte können – zum Zwecke der Archivierung oder für die Weiterbearbeitung mit anderen Programmen – ausgedruckt, in die Zwischenablage kopiert oder in eine Datei exportiert werden.

Die Dialogmasken des Logbuchs

Nach dem Aufruf des Logbuchs wird Ihnen im Dialog »Logbuch-Konfiguration« eine Übersicht der bereits gespeicherten Logbucheinträge angezeigt.

Durch einen Doppelklick auf einen Logbucheintrag wird die Detailansicht geöffnet.

Der Dialog »Logbuch-Konfiguration«

Im Dialog *Logbuch-Konfiguration* werden die bisher zu einem Gerät erfassten Logbucheinträge in Tabellenform aufgelistet.

Hier können Sie *Betreff* und *Status* (»Offen« oder »Erledigt«) sowie das *Datum* der letzten Bearbeitung jedes Eintrages sofort erkennen.

> **HINWEIS:** Die Sortierung der Tabelle erfolgt standardmäßig in absteigender Reihenfolge nach den Inhalten der Spalte »Status«. Dies wird durch ein kleines Dreieck im Kopf dieser Spalte angezeigt.
>
> Möchten Sie nach den Inhalten einer anderen Spalte sortieren, klicken Sie auf den Kopf der gewünschten Spalte. Ein weiterer Klick kehrt die Sortierreihenfolge um.

Folgende Aktionen sind im Logbuch möglich:

- **Hinzufügen:** Erstellung eines neuen Logbucheintrags
- **Ändern:** Aktualisierung eines bestehenden Logbucheintrags
- **Löschen:** Löschen eines Logbucheintrags
- **Drucken:** Logbucheintrag drucken
- **Exportieren:** Daten des Logbucheintrags in csv-Datei exportieren
- **Kopieren:** Details des Logbucheintrags in die Zwischenablage kopieren

Die Detailansicht eines Logbucheintrags

Die Detailansicht eines Logbucheintrages wird durch nach einem Doppelklick auf einen Eintrag angezeigt. Sie stellt Ihnen folgende Informationen zur Verfügung:

Betreff:	Kurztitel (max. 128 Zeichen), der in der Übersichtstabelle und dem Ausdruck einen schnellen Überblick erlaubt
Body:	detaillierte Beschreibung (max. 1.024 Zeichen)
Status:	aktueller Status (»Offen« bzw. »Erledigt«)
Ersteller:	Benutzername des Erstellers des Logbucheintrags
Erstellt:	Datum und Uhrzeit der ursprünglichen Erstellung
Letzter Bearbeiter:	Benutzername des Anwenders, der den Eintrag zuletzt geändert hat
Zuletzt bearbeitet:	Datum und Uhrzeit der letzten Änderung des Eintrags

Im oberen Teil des Dialogs sind einige besondere Schaltflächen angeordnet, die folgende Funkionalität bereitstellen:

- **(Pfeil links):** Anzeige des vorherigen Logbucheintrags (falls vorhanden)
- **Drucken:** Logbucheintrag drucken
- **Exportieren:** Daten des Logbucheintrags in csv-Datei exportieren
- **Kopieren:** Details des Logbucheintrags in die Zwischenablage kopieren
- **(Pfeil rechts):** Anzeige des nächsten Logbucheintrags (falls vorhanden)

HINWEIS: Die Funktionen der Schaltfächen *Drucken*, *Exportieren* und *Kopieren* entsprechen den gleichnamigen Einträgen im Kontextmenü der Logbucheinträge.

Diese Funktionen werden auf den folgenden Seiten erläutert.

Grundfunktionen des Logbuchs

Mit den Grundfunktionen des Logbuchs erstellen Sie neue oder bearbeiten bzw. löschen bereits erfasste Logbucheinträge.

WICHTIG: Für verschiedene Geräte innerhalb des KVM-Systems werden separate Logbücher geführt!

Erstellung eines neuen Logbucheintrags

So erstellen Sie einen neuen Eintrag im Logbuch eines Gerätes:

1. Klicken Sie im Strukturbaum auf den Ordner, der das Gerät enthält, dessen Logbuch Sie öffnen möchten.
2. Klicken Sie mit der rechten Maustaste auf das gewünschte Gerät und anschließend auf **Logbuch** im Kontextmenü.
3. Klicken Sie auf **Hinzufügen**.

4. Geben Sie den **Betreff** (max. 128 Zeichen) des Logbucheintrages ein.

> **TIPP:** Der Betreff wird in der Übersicht der Logbucheinträge angezeigt und erlaubt einen schnellen Überblick über die Einträge.

5. Geben Sie im Feld **Body** – falls gewünscht – eine detaillierte Beschreibung (max. 1.024 Zeichen) des Logbucheintrags ein.
6. Klicken Sie auf **OK**, um den neuen Eintrag im Logbuch zu speichern.

Änderung eines Logbucheintrages

So ändern Sie den Logbucheintrag eines Gerätes:

1. Klicken Sie im Strukturbaum auf den Ordner, der das Gerät enthält, dessen Logbuch Sie öffnen möchten.
2. Klicken Sie mit der rechten Maustaste auf das gewünschte Gerät anschließend auf **Logbuch** im Kontextmenü.
3. Klicken Sie auf den zu editierenden Eintrag und anschließend auf **Ändern**.
4. Ändern Sie ggf. den **Betreff** (max. 128 Zeichen) des Logbucheintrages ein.

> **TIPP:** Der Betreff wird in der Übersicht der Logbucheinträge angezeigt und erlaubt einen schnellen Überblick über die Einträge.

5. Ändern Sie ggf. im Feld **Body** die detaillierte Beschreibung (max. 1.024 Zeichen) des Logbucheintrags.
6. Wählen Sie im Feld **Status** zwischen den Optionen »Offen« und »Erledigt«.
7. Zu Ihrer Information werden in diesem Dialog zusätzlich folgende Informationen angezeigt:

Ersteller:	Name des Benutzers des KVM-Systems, der den Logbucheintrag erstellt hat
Erstellt:	Datum und Uhrzeit der ursprünglichen Erfassung des Eintrags
Letzter Bearbeiter:	Name des Benutzers des KVM-Systems, der den Logbucheintrag zuletzt geändert hat
Zuletzt bearbeitet:	Datum und Uhrzeit der letzten Änderung des Eintrags

8. Klicken Sie auf **OK**, um den Logbucheintrag zu speichern.

Löschen eines Logbucheintrages

So löschen Sie den Logbucheintrag eines Gerätes:

1. Klicken Sie im Strukturbaum auf den Ordner, der das Gerät enthält, dessen Logbuch Sie öffnen möchten.
2. Klicken Sie mit der rechten Maustaste auf das gewünschte Gerät anschließend auf **Logbuch** im Kontextmenü.
3. Klicken Sie auf den zu löschenden Eintrag und anschließend auf **Löschen**.
4. Bestätigen Sie die Sicherheitsabfrage durch Klick auf **Ja** oder brechen Sie den Vorgang durch Klick auf **Nein** ab.

Erweiterte Funktionen

Die erweiterten Funktionen erlauben Ihnen den Druck oder Export der Logbucheinträge. Alternativ können die Daten eines Logbucheintrages in die Zwischenablage kopiert werden.

Die erweiterten Funktionen können wahlweise über die Schaltflächen im Detail-Dialog des Logbuches aufgerufen werden. Alternativ können Sie diese Funktionen auch über das Kontextmenü des Dialog »Logbuch-Konfiguration« ausführen.

HINWEIS: Nur bei Aufruf der Funktionen über das Kontextmenü können die Funktionen auf mehrere Logbucheinträge gleichzeitig angewendet werden.

Drucken von Logbucheinträgen

So drucken Sie einen oder mehrere Logbucheinträge:

1. Klicken Sie im Strukturbaum auf den Ordner, der das Gerät enthält, dessen Logbuch Sie öffnen möchten.
2. Klicken Sie mit der rechten Maustaste auf das gewünschte Gerät anschließend auf **Logbuch** im Kontextmenü.
3. Markieren Sie einen oder mehrere der bereits erfassten Logbucheinträge.

   HINWEIS: Zur Auswahl mehrerer Logbucheinträge halten Sie die **Strg**-Taste gedrückt, während Sie die verschiedenen Einträge mit der Maus auswählen.

4. Klicken Sie mit der rechten Maustaste auf einen der markieren Einträge und anschließend auf **Drucken**.
5. Wählen Sie den **Drucker**, auf welchem das Dokument ausgegeben werden soll.

   HINWEIS: Falls gewünscht können Sie zusätzlich die Überschrift, die Anzahl der Kopien, das Seitenformat und die Randeinstellungen anpassen.

6. Klicken Sie auf **Drucken**.

Exportieren von Logbucheinträgen

Mit der Export-Funktion exportieren Sie die Daten eines Logbucheintrages in eine CSV-Datei.

Dieses Dateiformat wird üblicherweise für den Datenaustausch zwischen verschiedenen Programmen verwendet. Eine mit der Webapplikation *Config Panel* erstellte CSV-Datei kann beispielsweise mit allen gängigen Tabellenkalkulationsprogrammen eingelesen werden.

> **HINWEIS:** Die Abkürzung CSV steht für *Comma-Separated Values*.

So exportieren Sie einen oder mehrere Logbucheinträge:

1. Klicken Sie im Strukturbaum auf den Ordner, der das Gerät enthält, dessen Logbuch Sie öffnen möchten.
2. Klicken Sie mit der rechten Maustaste auf das gewünschte Gerät anschließend auf **Logbuch** im Kontextmenü.
3. Markieren Sie einen oder mehrere der bereits erfassten Logbucheinträge.

   > **HINWEIS:** Zur Auswahl mehrerer Logbucheinträge halten Sie die **Strg**-Taste gedrückt, während Sie die verschiedenen Einträge mit der Maus auswählen.

4. Klicken Sie mit der rechten Maustaste auf einen der markieren Einträge und anschließend auf **Exportieren**.
5. Wählen Sie im Bereich **Datei** des Dialogs, den Speicherort sowie den Dateinamen der zu erstellenden Datei.
6. Im Bereich Konfiguration haben Sie folgende Einstellungsmöglichkeiten:

Spaltenüberschriften:	Wählen Sie, ob die Spaltenüberschriften (*Betreff*, *Body*, …) in der CSV-Datei ausgegeben werden sollen. Optionen: **Ja**, **Nein**
Trennzeichen:	Wählen Sie das gewünschte Trennzeichen zwischen den verschiedenen Datenfeldern in der CSV-Datei. Optionen: **Tabulator**, **Semikolon**, **Komma**, **Leerzeichen**

7. Klicken Sie auf **Exportieren**.

Kopieren von Logbucheinträgen

Alternativ zur Export-Funktion, welche eine CSV-Datei erstellt, können Logbucheinträge mit der Kopieren-Funktion in die Zwischenablage des Betriebssystems kopiert werden.

Das Einfügen der kopierten Daten ist anschließend in jede Anwendung möglich, die auf die Zwischenablage zugreifen kann.

So kopieren Sie einen oder mehrere Logbucheinträge:

1. Klicken Sie im Strukturbaum auf den Ordner, der das Gerät enthält, dessen Logbuch Sie öffnen möchten.
2. Klicken Sie mit der rechten Maustaste auf das gewünschte Gerät anschließend auf **Logbuch** im Kontextmenü.
3. Markieren Sie einen oder mehrere der bereits erfassten Logbucheinträge.

   HINWEIS: Zur Auswahl mehrerer Logbucheinträge halten Sie die **Strg**-Taste gedrückt, während Sie die verschiedenen Einträge mit der Maus auswählen.

4. Klicken Sie mit der rechten Maustaste auf einen der markieren Einträge und anschließend auf **Kopieren**.
5. Öffnen Sie ein Dokument in der Anwendung, in welche Sie die Daten kopieren möchten, und betätigen Sie die Tastenkombination **Strg+V**.

Gemeinsames Editieren der Einstellungen

Die Webapplikation erlaubt das gemeinsame Editieren der Einstellungen durch zwei Benutzer mit entsprechenden Rechten.

Ändern zwei Benutzer die Einstellungen desselben Bereichs – beispielsweise die Einstellungen eines Benutzerkontos – so weist die Webapplikation durch folgende Markierungen auf die Änderungen durch den anderen Benutzer hin:

- Oberhalb der Schaltflächen des Dialogs erscheint die Meldung *Einstellungen wurden aktualisiert* in grüner Schrift.
- Die geänderte Einstellung und gegebenenfalls die Registerkarte, auf der diese Einstellung zu finden ist, wird ebenfalls in grüner Schrift dargestellt.

Sie haben folgende Möglichkeiten, die von Ihnen erfassten Daten zu verarbeiten:

Daten verwerfen:	1. Klicken Sie auf **Neu laden**, um die aktuellen Werte des Dialogs aus der Datenbank zu lesen.
Alle Daten überschreiben:	1. Klicken Sie auf **Übernehmen**. 2. Klicken Sie auf **Alle Daten überschreiben**.
Nur von Ihnen geänderte Werte speichern:	1. Klicken Sie auf **Übernehmen**. 2. Klicken Sie auf **Nur eigene Änderungen speichern**.

Benutzer und Gruppen

Effizienter Einsatz der Rechteverwaltung

Die Webapplikation verwaltet maximal 256 Benutzerkonten sowie die gleiche Anzahl an Benutzergruppen. Jeder Benutzer des Systems kann Mitglied von bis zu 20 Benutzergruppen sein.

Sowohl einem Benutzerkonto als auch einer Benutzergruppe können verschiedene Rechte innerhalb des Systems zugeordnet werden.

TIPP: Bei entsprechender Planung und Umsetzung der Benutzergruppen sowie der zugeordneten Rechte, ist es möglich, die Rechteverwaltung nahezu vollständig über die Benutzergruppen zu erledigen.

Änderungen an den Rechten der Benutzer können so besonders schnell und effizient durchgeführt werden.

Das Effektivrecht

Welche Berechtigung ein Benutzer für eine bestimmte Operation hat, wird anhand des Effektivrechts des Benutzers ermittelt.

WICHTIG: Das Effektivrecht ist das höchste Recht, das aus dem Individualrecht des Benutzerkontos und den Rechten der zugeordneten Gruppe(n) resultiert.

BEISPIEL: Der Benutzer *Muster* ist Mitglied der Gruppen *Office* und *TargetConfig*.

Die folgende Tabelle zeigt die Rechte des Benutzerkontos und der zugeordneten Gruppen sowie das daraus abgeleitete Effektivrecht:

Recht	Benutzer *Muster*	Gruppe *Office*	Gruppe *TargetConfig*	Effektivrecht
Target config	No	No	**Yes**	**Yes**
Change own password	No	**Yes**	No	**Yes**
Target access	**Full**	View	No	**Full**

Das Effektivrecht der Rechte *Target config* und *Change own password* resultieren aus den Rechten der Benutzergruppen. Das Recht *Target access*, welches in diesem Fall den Vollzugriff erlaubt, wurde hingegen direkt im Benutzerkonto vergeben.

In den Dialogmasken der Webapplikation wird hinter jeder Einstellung zusätzlich das Effektivrecht angezeigt.

TIPP: Klicken Sie in den Dialogen der Benutzerkonfiguration auf **Details**, um eine Auflistung der dem Benutzerkonto zugeordneten Gruppen sowie der dort vergebenen Rechte zu erhalten.

Effizienter Einsatz der Benutzergruppen

Durch den Einsatz von Benutzergruppen ist es möglich, für mehrere Benutzer mit identischen Kompetenzen, ein gemeinsames Rechteprofil zu erstellen und die Benutzerkonten der Mitgliederliste der Gruppe hinzuzufügen. Dies erspart die individuelle Konfiguration der Rechte der Benutzerkonten dieser Personen und erleichtert die Administration der Rechte innerhalb des Systems.

Werden die Rechte über Benutzergruppen gesteuert, so werden im Benutzerprofil ausschließlich die allgemeinen Daten des Benutzers sowie benutzerbezogene Einstellungen (Tastenkombinationen, Sprachauswahl, …) gespeichert.

Bei der Ersteinrichtung des Systems ist es empfehlenswert, verschiedene Gruppen für Anwender mit unterschiedlichen Kompetenzen einzurichten (z. B. *Office* und *IT*) und die entsprechenden Benutzerkonten zuzuordnen.

Ist eine weitere Differenzierung zwischen den Kompetenzen der Anwender erforderlich, können weitere Gruppen eingerichtet werden.

BEISPIEL: Sollen einige Benutzer der Gruppe *Office* die Berechtigung zum *Multi-Access*-Zugriff erhalten, bieten sich folgende Möglichkeiten an, dies mit Benutzergruppen zu realisieren:

- Sie erstellen eine Benutzergruppe (z. B. *Office_MultiAccess*), mit den identischen Einstellungen der Gruppe *Office*. Das Recht *Multi-Access* wird abschließend auf *full* gestellt. Ordnen Sie dieser Gruppe die entsprechenden Benutzerkonten zu.
- Sie erstellen eine Benutzergruppe (z. B. *MultiAccess*) und setzen ausschließlich das Recht *Multi-Access* auf *full*. Ordnen Sie dieser Gruppe die entsprechenden Benutzerkonten – *zusätzlich* zur Gruppe *Office* – zu.

In beiden Fällen erhält der Benutzer durch die Gruppen das Effektivrecht *full* für den *Multi-Access*-Zugriff.

HINWEIS: Möchten Sie einem Benutzer der Gruppe ein erweitertes Recht zuordnen, kann dies alternativ auch direkt im Benutzerprofil geändert werden.

Verwaltung von Benutzerkonten

Durch die Verwendung von Benutzerkonten besteht die Möglichkeit, die Rechte des Benutzers individuell festzulegen. Zusätzlich zu den Rechten können im persönlichen Profil einige benutzerbezogene Einstellungen festgelegt werden.

WICHTIG: Der Administrator sowie alle Benutzer mit aktiviertem *Superuser*-Recht sind berechtigt, Benutzer anzulegen, zu löschen und die Rechte sowie die benutzerbezogenen Einstellungen zu editieren.

Anlegen eines neuen Benutzerkontos

Die Webapplikation verwaltet maximal 256 Benutzerkonten. Jedes Benutzerkonto verfügt über individuelle Login-Daten, Rechte und benutzerbezogene Einstellungen für das KVM-System.

So erstellen Sie ein neues Benutzerkonto:

1. Klicken Sie im Strukturbaum auf **Benutzerbereich > Benutzer**.
2. Klicken Sie mit der rechten Maustaste in den Anzeigebereich und anschließend auf **Neu** im Kontextmenü.
3. Erfassen Sie folgende Daten innerhalb der Dialogmaske:

Name:	Geben Sie den gewünschten Benutzernamen ein.
Passwort:	Geben Sie das Passwort des Benutzerkontos ein.
Passwort wiederholen:	Wiederholen Sie das oben eingegebene Passwort.
Klartext:	Aktivieren Sie ggf. dieses Kontrollkästchen, um die beiden eingegebenen Passwörter im Klartext sehen und prüfen zu können.
Vollständiger Name:	Geben Sie hier – falls gewünscht – den vollständigen Namen des Benutzers ein.
Kommentar:	Erfassen Sie hier – falls gewünscht – einen beliebigen Kommentar zum Benutzerkonto.
Aktiviert:	Aktivieren Sie dieses Kontrollkästchen, um das Benutzerkonto zu aktivieren.

Ist das Benutzerkonto deaktiviert, wird dem Benutzer der Zugriff auf das KVM-System verweigert.

4. Klicken Sie auf **OK**, um die erfassten Daten zu speichern.

WICHTIG: Unmittelbar nach der Erstellung verfügt Benutzerkonto über keinerlei Rechte innerhalb des KVM-Systems.

Fügen Sie das Benutzerkonto einer bestehenden Benutzergruppe hinzu oder erteilen Sie dem Benutzerkonto individuelle Rechte (s. Seite 69).

Änderung des Namens eines Benutzerkontos

So ändern Sie den Namen eines Benutzerkontos:

1. Klicken Sie im Strukturbaum auf **Benutzerbereich > Benutzer**.
2. Klicken Sie mit der rechten Maustaste auf das zu editierende Benutzerkonto und anschließend auf **Konfiguration** im Kontextmenü.
3. Geben Sie im Feld **Name** den gewünschten Benutzernamen ein.
4. *Optional:* Geben Sie im Feld **Vollständiger Name** den vollständigen Namen des Benutzers ein.
5. Klicken Sie auf **OK**, um die erfassten Daten zu speichern.

Änderung des Passworts eines Benutzerkontos

So ändern Sie das Passwort eines Benutzerkontos:

1. Klicken Sie im Strukturbaum auf **Benutzerbereich > Benutzer**.
2. Klicken Sie mit der rechten Maustaste auf das zu konfigurierende Benutzerkonto und anschließend auf **Konfiguration** im Kontextmenü.
3. Klicken Sie auf **Passwort ändern**.
4. Ändern Sie folgende Daten innerhalb der Dialogmaske:

Neues Passwort:	Geben Sie das neue Passwort ein.
Passwort bestätigen:	Wiederholen Sie das oben eingegebene Passwort.
Klartext:	Aktivieren Sie dieses Kontrollkästchen, um die beiden eingegebenen Passwörter im Klartext sehen und prüfen zu können.

5. Zur Speicherung des neuen Passworts klicken Sie auf **OK**.
6. Klicken Sie auf **OK**, um die erfassten Daten zu speichern.

Änderung der Rechte eines Benutzerkontos

Den verschiedenen Benutzerkonten können differenzierte Berechtigungen erteilt werden.

Die folgende Tabelle listet die verschiedenen Berechtigungen auf. Weiterführende Hinweise zu den Rechten finden Sie auf den angegebenen Seiten.

Bezeichnung	Berechtigung	Seite
Change own password	Änderung des eigenen Passworts	Seite 74
Superuser right	Zugriff auf die Konfiguration des Systems uneingeschränkt möglich	Seite 73
WebIf login	Login mit der Webapplikation *Config Panel*	Seite 73

Änderung der Gruppenzugehörigkeit eines Benutzerkontos

HINWEIS: Jeder Benutzer des Systems kann Mitglied von bis zu 20 Benutzergruppen sein.

So ändern Sie die Gruppenzugehörigkeit eines Benutzerkontos:

1. Klicken Sie im Strukturbaum auf **Benutzerbereich > Benutzergruppen**.
2. Klicken Sie mit der rechten Maustaste auf die zu konfigurierende Benutzergruppe und anschließend auf **Konfiguration** im Kontextmenü.
3. Klicken Sie auf die Registerkarte **Mitglieder**.

   Hier haben Sie die Möglichkeit, Mitglieder der Benutzergruppe hinzuzufügen oder aus dieser zu entfernen.

   Der Dialog besteht aus zwei Tabellen, in welchen die Benutzerkonten des Systems aufgelistet werden:

Nicht zugeordnet:	Anzeige der Benutzerkonten, die dieser Gruppe *nicht* zugeordnet sind.
Zugeordnete Gruppenmitglieder:	Anzeige der Benutzerkonten, die dieser Gruppe zugeordnet sind.

4. Markieren Sie das Benutzerkonto, welches Sie der Gruppe hinzufügen oder aus dieser entfernen möchten.
5. Klicken Sie auf (*Pfeil rechts*), um das Benutzerkonto der Gruppe hinzuzufügen oder auf (*Pfeil links*), um dieses aus der Mitgliederliste zu entfernen.

Aktivierung oder Deaktivierung eines Benutzerkontos

WICHTIG: Ist das Benutzerkonto deaktiviert, wird dem Benutzer der Zugriff auf das KVM-System verweigert.

So aktivieren oder deaktivieren Sie ein Benutzerkonto:

1. Klicken Sie im Strukturbaum auf **Benutzerbereich > Benutzer**.
2. Klicken Sie mit der rechten Maustaste auf das zu (de)aktivierende Benutzerkonto und anschließend auf **Konfiguration** im Kontextmenü.
3. Aktivieren Sie das Kontrollkästchen **Aktiviert**, um das Benutzerkonto zu aktivieren.

   Möchten Sie den Zugang zum System mit diesem Benutzerkonto sperren, so deaktivieren Sie das Kontrollkästchen.
4. Klicken Sie auf **OK**, um die erfassten Daten zu speichern.

Löschen eines Benutzerkontos

So löschen Sie ein Benutzerkonto:

1. Klicken Sie im Strukturbaum auf **Benutzerbereich > Benutzer**.
2. Klicken Sie mit der rechten Maustaste auf das zu löschende Benutzerkonto und anschließend auf **Löschen** im Kontextmenü.
3. Bestätigen Sie die erscheinende Sicherheitsabfrage durch Klick auf **Ja** oder brechen Sie den Vorgang durch Klick auf **Nein** ab.

Verwaltung von Benutzergruppen

Durch den Einsatz von *Benutzergruppen* ist es möglich, für mehrere Benutzer mit identischen Kompetenzen ein gemeinsames Rechteprofil zu erstellen und die Benutzerkonten als Mitglieder dieser Gruppe hinzuzufügen.

Dies erspart die individuelle Konfiguration der Rechte von Benutzerkonten dieser Personen und erleichtert die Administration der Rechte innerhalb des KVM-Systems.

HINWEIS: Der Administrator sowie alle Benutzer mit aktiviertem *Superuser*-Recht sind berechtigt, Benutzergruppen anzulegen, zu löschen und die Rechte sowie die Mitgliederliste zu editieren.

Anlegen einer neuen Benutzergruppe

Innerhalb des Systems können Sie bis zu 256 Benutzergruppen erstellen.

So erstellen Sie eine neue Benutzergruppe:

1. Klicken Sie im Strukturbaum auf **Benutzerbereich > Benutzergruppen**.
2. Klicken Sie mit der rechten Maustaste in den Anzeigebereich und anschließend auf **Neu** im Kontextmenü.

3. Erfassen Sie folgende Daten innerhalb der Dialogmaske:

Name:	Geben Sie den gewünschten Namen der Benutzergruppe ein.
Aktiviert:	Aktivieren Sie dieses Kontrollkästchen, um die Benutzergruppe zu aktivieren. **HINWEIS:** Ist die Benutzergruppe deaktiviert, wirken sich die Rechte der Gruppe *nicht* auf die zugeordneten Mitglieder aus.
Kommentar:	Erfassen Sie hier – falls gewünscht – einen beliebigen Kommentar zur Benutzergruppe.

4. Klicken Sie auf **OK**, um die erfassten Daten zu speichern.

WICHTIG: Unmittelbar nach der Erstellung verfügt die Benutzergruppe über keinerlei Rechte innerhalb des Systems.

Änderung des Namens einer Benutzergruppe

So ändern Sie den Namen einer Benutzergruppe:

1. Klicken Sie im Strukturbaum auf **Benutzerbereich > Benutzergruppen**.
2. Klicken Sie mit der rechten Maustaste auf das zu editierende Benutzerkonto und anschließend auf **Konfiguration** im Kontextmenü.
3. Geben Sie im Feld **Name** den gewünschten Namen der Benutzergruppe ein.
4. Klicken Sie auf **OK**, um die erfassten Daten zu speichern.

Änderung der Rechte einer Benutzergruppe

Den verschiedenen Benutzergruppen können differenzierte Berechtigungen erteilt werden.

Die folgende Tabelle listet die verschiedenen Berechtigungen auf. Weiterführende Hinweise zu den Rechten finden Sie auf den angegebenen Seiten.

Bezeichnung	Berechtigung	Seite
Change own password	Änderung des eigenen Passworts	Seite 74
Superuser right	Zugriff auf die Konfiguration des Systems uneingeschränkt möglich	Seite 73
WebIf login	Login mit der Webapplikation *Config Panel*	Seite 73

Mitgliederverwaltung einer Benutzergruppe

So verwalten Sie die Mitglieder einer Benutzergruppe:

1. Klicken Sie im Strukturbaum auf **Benutzerbereich > Benutzergruppen**.
2. Klicken Sie mit der rechten Maustaste auf die zu editierende Benutzergruppe und anschließend auf **Konfiguration** im Kontextmenü.
3. Klicken Sie auf die Registerkarte **Mitglieder**.

   Hier haben Sie die Möglichkeit, Mitglieder der Benutzergruppe hinzuzufügen oder aus dieser zu entfernen.

   Der Dialog besteht aus zwei Tabellen, in welchen die Benutzerkonten des KVM-Systems aufgelistet werden:

Nicht zugeordnet:	Anzeige von Benutzerkonten, die dieser Gruppe *nicht* zugeordnet sind.
Zugeordnete Gruppenmitglieder:	Anzeige von Benutzerkonten, die dieser Gruppe zugeordnet sind.

4. Markieren Sie das Benutzerkonto, welches Sie der Gruppe hinzufügen oder aus dieser entfernen möchten.
5. Klicken Sie auf (*Pfeil rechts*), um das Benutzerkonto der Gruppe hinzuzufügen oder auf (*Pfeil links*), um dieses aus der Mitgliederliste zu entfernen.

Aktivierung oder Deaktivierung einer Benutzergruppe

So aktivieren oder deaktivieren Sie eine Benutzergruppe:

1. Klicken Sie im Strukturbaum auf **Benutzerbereich > Benutzergruppen**.
2. Klicken Sie mit der rechten Maustaste auf die zu (de)aktivierende Benutzergruppe und anschließend auf **Konfiguration** im Kontextmenü.
3. Aktivieren Sie das Kontrollkästchen **Aktiviert**, um die Benutzergruppe zu aktivieren.

   Möchten Sie den Mitgliedern der Benutzergruppe den Zugang zum KVM-System sperren, so deaktivieren Sie das Kontrollkästchen.

4. Klicken Sie auf **OK**, um die erfassten Daten zu speichern.

Löschen einer Benutzergruppe

So löschen Sie eine Benutzergruppe:

1. Klicken Sie im Strukturbaum auf **Benutzerbereich > Benutzergruppen**.
2. Klicken Sie mit der rechten Maustaste auf die zu löschende Benutzergruppe und anschließend auf **Löschen** im Kontextmenü.
3. Bestätigen Sie die erscheinende Sicherheitsabfrage durch Klick auf **Ja** oder brechen Sie den Vorgang durch Klick auf **Nein** ab.

Systemrechte

Berechtigung zum uneingeschränkten Zugriff (Superuser)

Das *Superuser*-Recht erlaubt einem Benutzer den uneingeschränkten Zugriff auf die Konfiguration des KVM-Systems.

HINWEIS: Die Informationen über die zuvor zugewiesenen Rechte des Benutzers bleiben bei der Aktivierung des *Superuser*-Rechtes weiterhin gespeichert und werden bei Entzug des Rechtes wieder aktiviert.

So ändern Sie die Berechtigung zum uneingeschränkten Zugriff:

1. Möchten Sie dieses Recht eines Benutzerkontos ändern, klicken Sie im Strukturbaum auf **Benutzerbereich > Benutzer**.

   Im Falle einer Benutzergruppe klicken Sie auf **Benutzerbereich > Benutzergruppen**.
2. Klicken Sie im Anzeigebereich mit der rechten Maustaste auf das zu konfigurierende Benutzerkonto bzw. die Benutzergruppeund anschließend auf **Konfiguration** im Kontextmenü.
3. Klicken Sie auf den Reiter **System-Rechte**.
4. Wählen Sie im Feld **Superuser-Recht** zwischen folgenden Optionen:

Ja:	Uneingeschränkten Zugriff auf das KVM-System und die angeschlossenen Geräte erlaubt
Nein:	Uneingeschränkten Zugriff auf das KVM-System und die angeschlossenen Geräte untersagt

5. Klicken Sie auf **OK**, um die erfassten Daten zu speichern.

Berechtigung zum Login in die Webapplikation

So ändern Sie die Berechtigung zum Login mit der Webapplikation:

1. Möchten Sie dieses Recht eines Benutzerkontos ändern, klicken Sie im Strukturbaum auf **Benutzerbereich > Benutzer**.

   Im Falle einer Benutzergruppe klicken Sie auf **Benutzerbereich > Benutzergruppen**.
2. Doppelklicken Sie auf das zu konfigurierende Benutzerkonto bzw. die Benutzergruppe.
3. Klicken Sie auf den Reiter **System-Rechte**.
4. Wählen Sie im Feld **Web-Interface Login** zwischen folgenden Optionen:

Ja:	Zugriff auf die Webapplikation erlaubt
Nein:	Zugriff auf die Webapplikation untersagt

5. Klicken Sie auf **OK**, um die erfassten Daten zu speichern.

Berechtigung zur Änderung des eigenen Passworts

So ändern Sie die Berechtigung zur Änderung des eigenen Passworts:

1. Möchten Sie dieses Recht eines Benutzerkontos ändern, klicken Sie im Strukturbaum auf **Benutzerbereich > Benutzer**.

   Im Falle einer Benutzergruppe klicken Sie auf **Benutzerbereich > Benutzergruppen**.

2. Klicken Sie im Anzeigebereich mit der rechten Maustaste auf das zu konfigurierende Benutzerkonto bzw. die Benutzergruppe und anschließend auf **Konfiguration** im Kontextmenü.

3. Klicken Sie auf die Reiter **System-Rechte**.

4. Wählen Sie im Feld **Eigenes Passwort ändern** zwischen folgenden Optionen:

Ja:	Passwortänderung des eigenen Benutzerkontos erlaubt
Nein:	Passwortänderung des eigenen Benutzerkontos untersagt

5. Klicken Sie auf **OK**, um die erfassten Daten zu speichern.

Der Ordner »KVM-Kombinationen«

Im Ordner *KVM-Kombinationen* können Sie verschiedene Geräte in beliebigen Ordnern gruppieren. Speziell in größeren Systemen haben Sie so die Möglichkeit, einen guten Überblick zu bewahren.

Sie können die Geräte beispielsweise nach Standorten (z. B. Serverraum) oder nach beliebigen anderen Merkmalen (z. B. Betriebssystem des angeschlossenen Computers) gruppieren.

TIPP: Innerhalb eines Ordners können Sie Geräte *verschiedener* Klassen – beispielsweise Target-Module eines Matrixsystems oder Extender – gruppieren.

Ordnerverwaltung

Im Ordner *KVM-Kombinationen* sind folgende Systemordner enthalten:

[Nicht zugeordnet]:	In diesem Ordner werden alle Geräte aufgeführt, die bisher keiner KVM-Kombination zugeordnet sind.
[Alle Geräte]:	In diesem Ordner werden alle Geräte des KVM-Systems aufgelistet.

HINWEIS: Die Systemordner können weder gelöscht noch umbenannt werden.

Erstellen eines neuen Ordners

So erstellen Sie einen leeren Ordner:

1. Klicken Sie im Strukturbaum mit der rechten Maustaste auf **KVM-Kombinationen** und anschließend auf **Neuer Ordner** im Kontextmenü.

   TIPP: Möchten Sie einen Unterordner erstellen, klicken Sie im Kontextmenü des übergeordneten Ordners auf den Eintrag **Neuer Ordner**.

2. Geben Sie im Feld **Name** die gewünschte Bezeichnung ein.
3. *Optional:* Geben Sie im Feld **Kommentar** einen Kommentar ein.
4. Klicken Sie auf **OK**, um den Ordner zu erstellen.

Ein Gerät einem Ordner zuordnen

HINWEIS: Jedes Gerät kann in beliebig vielen Unterordnern enthalten sein.

So gruppieren Sie *verbundene Geräte* in einem neuen Ordner:

1. Klicken Sie im Strukturbaum auf **KVM-Kombinationen > [Alle Geräte]**.
2. Klicken Sie mit der rechten Maustaste auf ein Gerät eines Verbundes und anschließend auf **Verbundene Geräte gruppieren** im Kontextmenü.
3. Geben Sie im Feld **Name** die gewünschte Bezeichnung des neuen Ordners ein.
4. *Optional:* Geben Sie im Feld **Kommentar** einen Kommentar ein.
5. Klicken Sie auf **OK**, um die Geräte im neuen Ordner zu gruppieren.

So ordnen Sie ein Gerät einem bestehenden Ordner zu:

1. Klicken Sie im Strukturbaum auf **KVM-Kombinationen > [Alle Geräte]**.
2. Klicken Sie mit der rechten Maustaste auf das zuzuordnende Gerät und anschließend auf **Gerät kopieren** im Kontextmenü.
3. Öffnen Sie den Ordner, welcher das Gerät zugeordnet werden soll.
4. Klicken Sie in der Hauptansicht mit der rechten Maustaste und anschließend auf **Gerät einfügen** im Kontextmenü.

Ein Gerät aus einem Ordner entfernen

Das Entfernen eines Gerätes aus einem Ordner kann wahlweise durch das Verschieben des Gerätes in die Gruppe *[Nicht zugeordnet]* oder durch Auswahl des Eintrags **Aus Position entfernen** im Kontextmenü erreicht werden.

So heben Sie die Zuordnung eines Target-Moduls zu einem Ordner auf:

1. Klicken Sie im Strukturbaum auf **KVM-Kombinationen > [Alle Geräte]**.
2. Öffnen Sie den Ordner, welcher das Gerät aktuell zugeordnet ist.

   Klicken Sie mit der rechten Maustaste auf das Gerät, dessen Zuordnung Sie löschen möchten und anschließend auf **Aus Position entfernen** im Kontextmenü.

Umbenennen eines Ordners

So benennen Sie einen Ordner um:

1. Klicken Sie im Strukturbaum auf **KVM-Kombinationen > [Alle Geräte]**.
2. Klicken Sie mit der rechten Maustaste auf den umzubenennenden Ordner und anschließend auf **Ordner umbenennen** im Kontextmenü.
3. Editieren Sie den Namen und betätigen Sie die **Eingabetaste**.

Löschen eines Ordners

Von Ihnen erstellte Ordner können jederzeit gelöscht werden.

Beinhaltet ein Ordner während des Löschvorgangs Geräte, werden diese automatisch in die Gruppe *[Nicht zugeordnet]* verschoben.

HINWEIS: Die Systemordner *[Nicht zugeordnet]* und *[Alle Geräte]* werden durch die Webapplikation verwaltet und können *nicht* gelöscht werden.

So löschen Sie einen Ordner:

1. Klicken Sie im Strukturbaum auf **KVM-Kombinationen > [Alle Geräte]**.
2. Klicken Sie mit der rechten Maustaste auf den zu löschenden Ordner und anschließend auf **Ordner löschen** im Kontextmenü.

   HINWEIS: Die Mehrfachauswahl von Ordnern ist bei gleichzeitiger Betätigung der **Shift**- bzw. der **Strg**-Taste mit der linken Maustaste möglich.

3. Bestätigen Sie die erscheinende Sicherheitsabfrage durch Klick auf **Ja** oder brechen Sie den Vorgang durch Klick auf **Nein** ab.

Erweiterte Funktionen des KVM-Systems

SNMP-Traps der Geräte temporär unterdrücken (Wartungsmodus)

Durch Aktivierung des Wartungsmodus (*Maintenance*-Modus) können Sie die Aussendung von SNMP-Traps (s. Seite 54) von Geräten, an welchen beispielsweise Installationsarbeiten durchgeführt werden, gezielt deaktivieren.

Nach Abschluss der Installationsarbeiten und Deaktivierung des Wartungsmodus werden die Statusmeldungen wieder angezeigt bzw. gemeldet.

Aktivierung bzw. Deaktivierung des Wartungsmodus

So (de)aktivieren Sie den Wartungsmodus eines Gerätes:

1. Klicken Sie im Strukturbaum auf **UserCenter**.
2. Klicken Sie mit der rechten Maustaste auf das Gerät und anschließend auf **Wartung > An** bzw. **Wartung > Aus** im Kontextmenü.

Auflistung der Geräte im Wartungsmodus einsehen

So zeigen Sie die Auflistung der Geräte im Wartungsmodus an:

1. Klicken Sie im Strukturbaum auf die Ordner **Systemüberwachung > Wartung**.

   In der Hauptansicht werden die entsprechenden Geräte aufgelistet.

   TIPP: In *allen* Ansichten werden Geräte im Wartungsmodus gelb hinterlegt dargestellt.

Identifizierung eines Gerätes durch Aktivierung der Identification-LED

Einige Geräte sind mit einer *Identification*-LED an der Frontblende ausgestattet.

Über die Webapplikation können Sie die LEDs der Geräte ein- bzw. ausschalten, um die Geräte beispielsweise innerhalb eines Racks zu identizieren.

So (de)aktivieren Sie die *Identification*-LED eines Gerätes:

1. Klicken Sie im Strukturbaum auf **UserCenter**.
2. Klicken Sie mit der rechten Maustaste auf das Gerät und anschließend auf **Identification-LED > An** bzw. **Identification-LED > Aus** im Kontextmenü.

Sicherung und Wiederherstellung der Daten des KVM-Systems

Alle Konfigurationseinstellungen können über die Backup-Funktion gesichert werden. Das Wiederherstellen der gesicherten Daten ist über die Restore-Funktion möglich.

TIPP: Die Sicherung sowie die Wiederherstellung der Konfiguration können Sie wahlweise über den Eintrag **System > Werkzeuge** im Strukturbaum oder über das **Werkzeugsymbol > Werkzeuge** starten.

So sichern Sie die Konfigurationseinstellungen des KVM-Systems:

1. Klicken Sie im Strukturbaum auf **System > Werkzeuge**.
2. Klicken Sie auf **Backup**.
3. Geben Sie im Feld **Pfad** den Speicherort und den Namen der Backup-Datei an.

   TIPP: Verwenden Sie die Datei-Schaltfläche, um den Speicherort und den Namen der Backup-Datei über den Datei-Dialog auszuwählen.

4. *Optional:* Erfassen Sie ein **Passwort** zur Sicherung der Backup-Datei und/oder einen **Kommentar** .
5. Wählen Sie den Umfang der zu speichernden Daten: Sie können wahlweise die **Netzwerk-Einstellungen** und/oder die **Anwendungs-Einstellungen** sichern.
6. Klicken Sie auf **Backup**.

So stellen Sie die Konfigurationseinstellungen des KVM-Systems wieder her:

1. Klicken Sie im Strukturbaum auf **System > Werkzeuge**.
2. Klicken Sie auf **Restore**.
3. Geben Sie im Feld **Pfad** den Speicherort und den Namen der Backup-Datei an.

   TIPP: Verwenden Sie die Datei-Schaltfläche, um den Speicherort und den Namen der Backup-Datei über den Datei-Dialog auszuwählen.

4. Prüfen Sie anhand der Informationen der Felder **Erstellungs-Datum** und **Kommentar** des Dialogs, ob es sich um die gewünschten Backup-Datei handelt.

5. Wählen Sie den Umfang der zu wiederherzustellenden Daten: Sie können wahlweise die **Netzwerk-Einstellungen** und/oder die **Anwendungs-Einstellungen** wiederherstellen.

   HINWEIS: Falls während der Sicherung der Daten einer der Bereiche ausgelassen wurde, ist dieser Bereich nicht anwählbar.

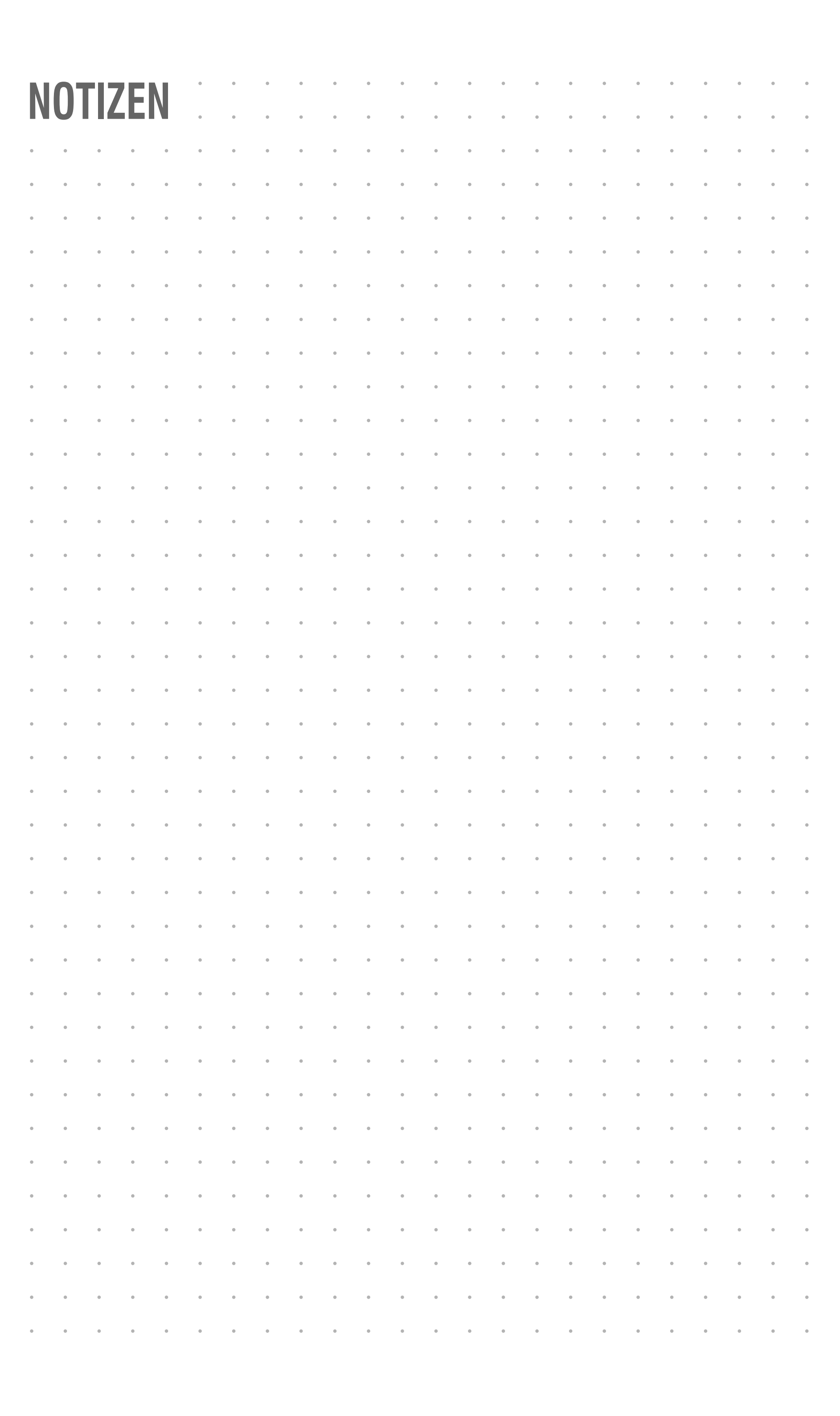
6. Klicken Sie auf **Restore**.
7. Klicken Sie auf **OK**, um den Dialog zu verlassen.

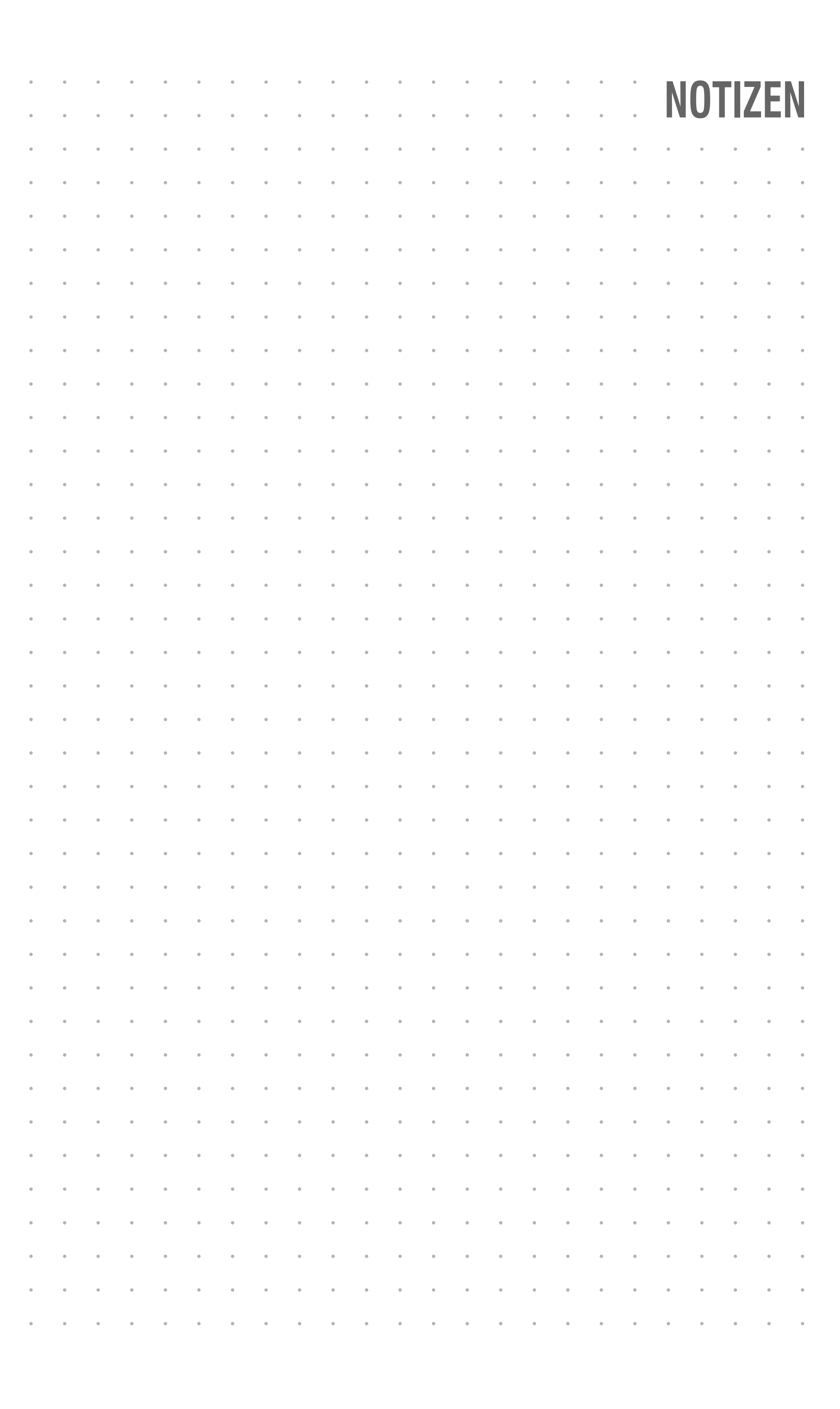
Übersicht der Monitoring-Werte

In den gerätespezifischen Zweigen sowie in den Zweigen *KVM-Kombinationen* und *Kritische Geräte* des Strukturbaums können Sie aktuelle Statusinformationen des Gerätes einsehen.

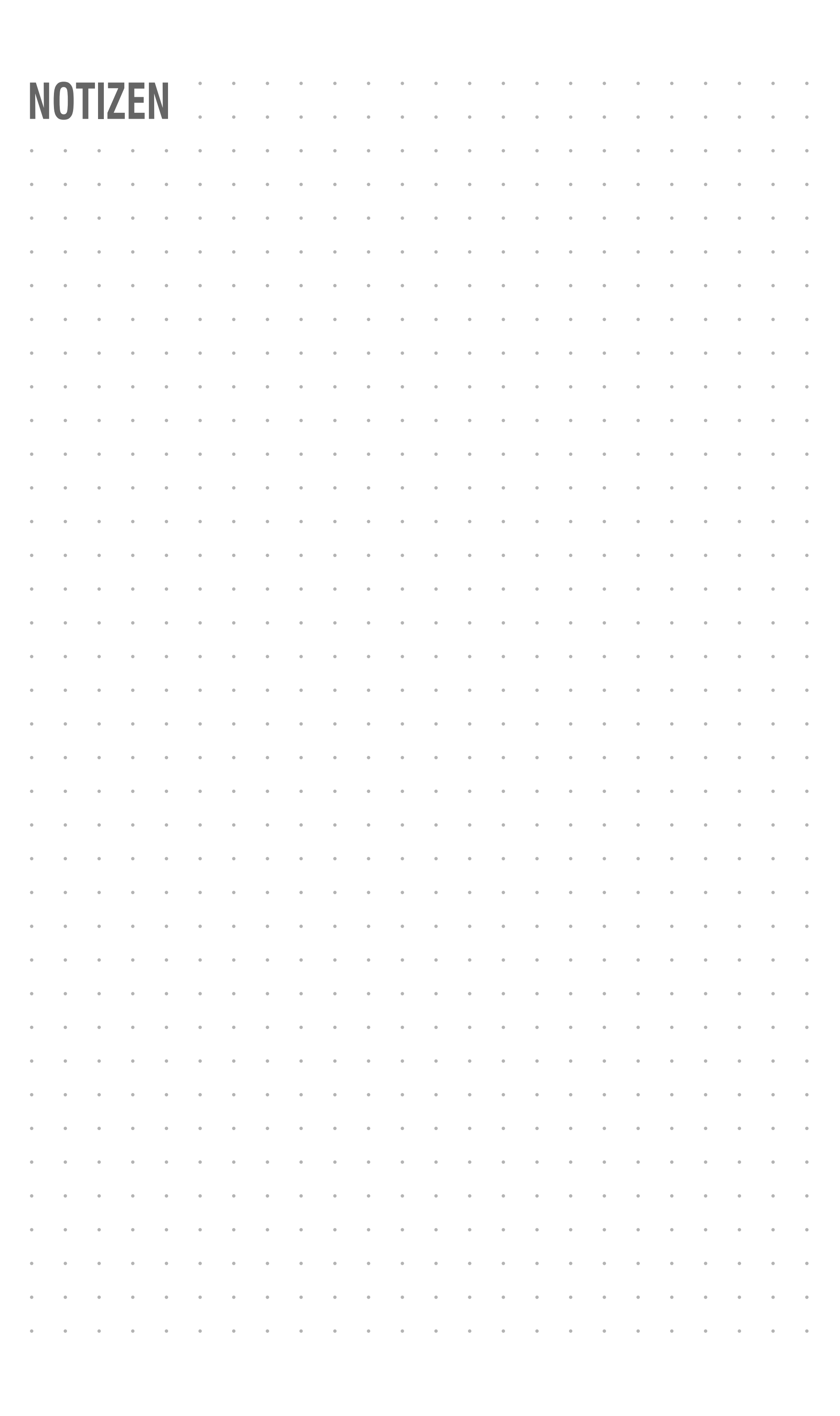
Eigenschaft	Status	Bedeutung
Lüfter-geschwindigkeit	Zahlenwert	Umdrehungszahl (rpm) des Lüfters
Main power	On	Stromversorgung über Netzteil »Main power« hergestellt
	Off	Stromversorgung über Netzteil »Main power« getrennt
Network A	Down	Verbindung zum Netzwerk getrennt
	Up	Verbindung zum Netzwerk hergestellt
Network B	Down	Verbindung zum Netzwerk getrennt
	Up	Verbindung zum Netzwerk hergestellt
Red. power	On	Stromversorgung über Netzteil »Red. power« hergestellt
	Off	Stromversorgung über Netzteil »Red. power« getrennt
Temperatur	Zahlenwert	Anzeige der aktuellen Temperatur (°C) im Gerät

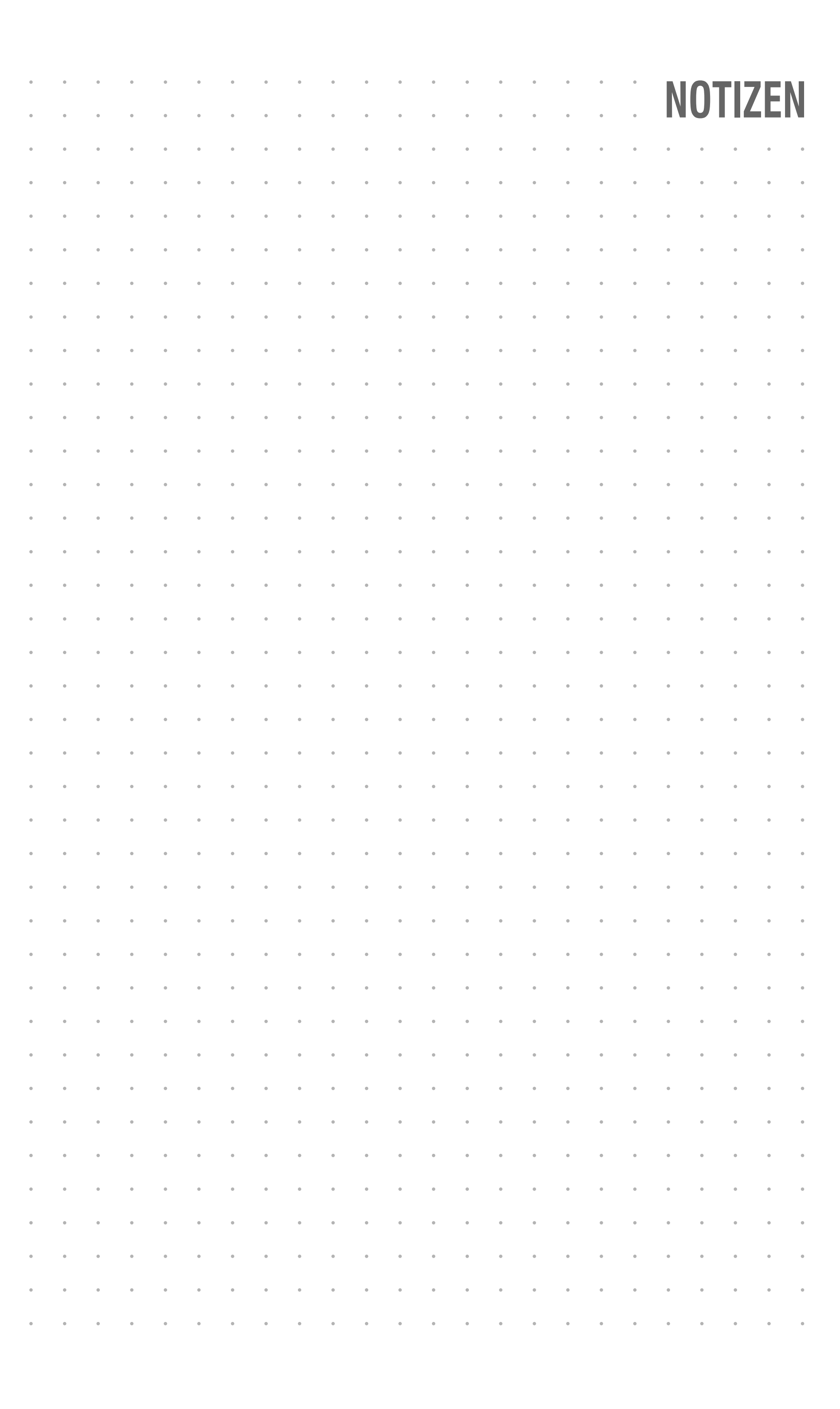
NOTIZEN




NOTIZEN

NOTIZEN





NOTIZEN



Das Handbuch wird fortlaufend aktualisiert und im Internet veröffentlicht.

http://gdsys.de/A9100194

Guntermann & Drunck GmbH

Dortmunder Str. 4a
57234 Wilnsdorf

Germany

http://www.GDsys.de
sales@GDsys.de

